



# Department of Homeland Security

## Information Analysis and Infrastructure Protection Directorate

### CyberNotes

*Issue #2004-04*

*February 23, 2004*

***We are beginning the process of integrating CyberNotes into the US-CERT product line. Notice of impending changes will be sent to the CyberNotes Distribution List as they become available.***

CyberNotes is published every two weeks by the Department of Homeland Security/Information Analysis and Infrastructure Protection (IAIP) Directorate/ National Cyber Security Division (NCSD). 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 Department of Homeland Security US-CERT web site at <http://www.us-cert.gov>.

### ***Bugs, Holes & Patches***

The following table provides a summary of software vulnerabilities identified between February 3 and February 23, 2004. 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
ACLogic <sup>1</sup>	Windows	CesarFTP 0.99 e	A remote Denial of Service vulnerability exists due to a failure to handle multiple sessions when a long string is retrieved.	No workaround or patch available at time of publishing.	CesarFTP Remote Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

<sup>1</sup> Bugtraq, February 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ai Graphics & Joe Lumbroso <sup>2</sup>	Windows, Unix	Jacks FormMail .php 2.0, 5.0	A vulnerability exists due to insufficient validation in the 'check_referrer()' function, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Jack's Formmail.php Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
AIM Sniff <sup>3</sup>	Unix	AIM Sniff 0.6-0.9	A vulnerability exists in the 'aimSniff.pl' script because a temporary log file is created insecurely without verifying if the file already exists, which could let a malicious user obtain elevated privileges.	Upgrades available at: <a href="http://prdownloads.sourceforge.net/aimsniff/aimsniff-0.9d.tar.gz?download">http://prdownloads.sourceforge.net/aimsniff/aimsniff-0.9d.tar.gz?download</a>	AIM Sniff Insecure Temporary File Creation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Apache-ssl.org <sup>4</sup>	Unix	Apache-SSL 1.3.28+ 1.52 & prior	A vulnerability exists in the 'SSLFakeBasicAuth' mode when processing client-side certificates, which could let a remote malicious user forge a valid client certificate.	Upgrade available at: <a href="http://www.apache-ssl.org/">http://www.apache-ssl.org/</a>	Apache-SSL Client Certificate Forging	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
APC <sup>5</sup>	Multiple	WEB/SNMP Management Card (9606) Firmware 3.0, 3.0.1	A vulnerability exists because the management cards used for factory initialization include a common 'backdoor' password, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: <a href="http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch">http://www.apc.com/go/direct/index.cfm?tag=sa2988_patch</a>	SmartSlot Web/SNMP Management Card Default Password	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

<sup>2</sup> Secunia Advisory, SA10815, February 9, 2004.

<sup>3</sup> Securiteam, February 16, 2004.

<sup>4</sup> Bugtraq, February 6, 2004.

<sup>5</sup> APC Security Advisory, February 19, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
ASP Portal <sup>6</sup>	Windows	ASP Portal	Multiple vulnerabilities exist: a vulnerability exists due to insufficient sanitization of user-supplied data that is incorporated into dynamic content, which could let a remote malicious user execute arbitrary HTML code; a vulnerability exists in the 'index.asp' page due to insufficient sanitization of URI parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists in the 'index.asp' script due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists due to insufficient sanitization when collecting user-supplied data from cookie parameters that will be later incorporated into an SQL query statement, which could let a remote malicious user provide malicious SQL statements as a value for the affected cookie parameter; and a vulnerability exists due to the way methods are used to store session cookies because user names associated with the current session are stored in plaintext, which could let a remote malicious user obtain sensitive information.	Upgrade available at: <a href="http://www.aspportal.net/downloadsviewer.asp?theurl=38">http://www.aspportal.net/downloadsviewer.asp?theurl=38</a>	Multiple ASP Portal Vulnerabilities	<b>Medium/High</b>  <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published. An exploit script has been published for the Cookie Account Hijack vulnerability.
BolinTech <sup>7</sup>	Windows, Unix	Dream FTP Server 1.02	A format string vulnerability exists in 'Server Log' when log information is displayed, 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.	BolinTech Dream FTP Server User Name Format String	<b>Low/High</b>  <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>6</sup> Bugtraq, February 14, 2004.

<sup>7</sup> SP Research Labs Advisory x09, February 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
BosDev, Inc. <sup>8</sup>	Windows, Unix	BosDates 3.0-3.2	A vulnerability exists in the 'calendar_download.php' script due to insufficient validation of user-supplied input in the 'calendar' parameter, which could let a remote malicious user obtain sensitive information.	Patch available at: <a href="http://www.bosdev.com/support/">http://www.bosdev.com/support/</a>	BosDates Input Validation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Brad Fears <sup>9</sup>	Unix	PhpCode Cabinet 0.2-0.4	Vulnerabilities exist in various scripts due to insufficient verification of certain parameters, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrades available at: <a href="http://prdownloads.sourceforge.net/phpcodecabinet/phpc-0.5.tar.gz?download">http://prdownloads.sourceforge.net/phpcodecabinet/phpc-0.5.tar.gz?download</a>	PHPCode Cabinet Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Brad Fears <sup>10</sup>	Unix	PhpCode Cabinet 0.1-0.4	Cross-Site Scripting vulnerabilities exist because several scripts do not properly validate user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: <a href="http://prdownloads.sourceforge.net/phpcodecabinet/phpc-0.5.tar.gz">http://prdownloads.sourceforge.net/phpcodecabinet/phpc-0.5.tar.gz</a>	PHPCode Cabinet Multiple Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Cactusoft Ltd. <sup>11</sup>	Windows	Cactu Shop Lite 5.0	A backdoor vulnerability exists in the 'strEmailAddress' variable, which could let a remote malicious user delete arbitrary files and cause a Denial of Service. <i>Note: The vendor reportedly confirms that the Lite version of the product includes backdoors but indicates that the Lite version is not intended for live use.</i>	No workaround or patch available at time of publishing.	CactuShop Lite Remote Arbitrary File Deletion Backdoor	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Caucho Technology <sup>12</sup>	Windows NT 4.0/2000	Resin 2.1.12	An information disclosure vulnerability exists which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Resin Information & Directory Listing Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

<sup>8</sup> Secunia Advisory, SA10844, February 11, 2004.

<sup>9</sup> Secunia Advisory, SA10862, February 12, 2004.

<sup>10</sup> SecurityFocus, February 11, 2004.

<sup>11</sup> S-Quadra Advisory, February 6, 2004.

<sup>12</sup> Bugtraq, February 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
clamav. Source forge.net <sup>13</sup>	Unix	Clam Anti- Virus ClamAV 0.65	A remote Denial of Service vulnerability exists when a malicious user submits a malformed UUEncoded message.	Patch available at:  <a href="http://cvs.sourceforge.net/viewcvs.py/clamav/clamav-devel/libclamav/message.c">http://cvs.sourceforge.net/viewcvs.py/clamav/clamav-devel/libclamav/message.c</a>	ClamAV Daemon Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Computer Associates <sup>14</sup>	Unix	Inoculate IT 6.0	Multiple vulnerabilities exist: a vulnerability exists in the 'inoregupdate,' 'uniftest,' and 'unimove' scripts because temporary files are created insecurely, which could let a malicious user overwrite, create, and delete arbitrary files; and a vulnerability exists because some directories are installed with insecure default permissions, which could let a malicious user modify sensitive information.	No workaround or patch available at time of publishing.	InoculateIT Insecure Default Installation	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Computer Associates <sup>15</sup>	Windows	eTrust Antivirus EE 7.0	A vulnerability exists because the scanning engine does not handle ZIP archives containing password protected files correctly, which could let remote malicious user send a virus through the antiviral system without detection.	Patch available at:  <a href="ftp://ftp.ca.com/pub/unicenter/eTrust/AntiVirus/7.0/nt/q050563/QO50563.CAZ">ftp://ftp.ca.com/pub/unicenter/eTrust/AntiVirus/7.0/nt/q050563/QO50563.CAZ</a>	eTrust Antivirus Password Protected Zip File	High	Bug discussed in newsgroups and websites. There is no exploit code required.
Crob Software Studio <sup>16</sup>	Windows NT	Crob FTP Server 3.5.2	A remote Denial of Service vulnerability exists when a malicious user connects and disconnects from the FTP service without submitting any data.	No workaround or patch available at time of publishing.	Crob FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
<b>Debian</b> <sup>17</sup>  <i>More vendors issue advisories 18, 19, 20</i>	Unix	<b>GNU/ Linux unstable alias sid, GNU/ Linux 3.0</b>	<b>A vulnerability exists in 'netpnm' because temporary files are created in an insecure manner, which could let a malicious user obtain elevated privileges.</b>	<b>Debian:</b>  <a href="http://security.debian.org/pool/updates/main/n/netpnm-free/">http://security.debian.org/pool/updates/main/n/netpnm-free/</a>  <b>Mandrake:</b>  <a href="http://www.mandrakesecurity.net/en/advisories/">http://www.mandrakesecurity.net/en/advisories/</a> <b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/i386/">ftp://updates.redhat.com/9/en/os/i386/</a> <b>SGI:</b>  <a href="ftp://patches.sgi.com/support/free/security/advisories">ftp://patches.sgi.com/support/free/security/advisories</a>	<b>Netpbm Temporary File</b>  <b>CVE Name: CAN-2003- 0924</b>	Medium	<b>Bug discussed in newsgroups and websites.</b>

<sup>13</sup> Secunia Advisory, SA10826, February 10, 2004.

<sup>14</sup> Secunia Advisory, SA10833, February 10, 2004.

<sup>15</sup> Computer Associates, APAR #: QO50563, February 13, 2004.

<sup>16</sup> Bugtraq, February 12, 2004.

<sup>17</sup> Debian Security Advisory DSA 426-1, January 17, 2004.

<sup>18</sup> Red Hat Security Advisories, RHSA-2004:030-01 & RHSA-2004:031-02, February 3 & 5, 2004.

<sup>19</sup> SGI Security Advisory, 20040201-01-U, February 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Early Impact <sup>21</sup>	Windows	Product Cart 1.5, 1.6 br, br001, br003, 1.6 b, b001-b003, 1.5002, 1.5003, 1.5003 r, 1.5004, 1.6002, 1.6003, 2.0, 2.0 br000, 2.5	Multiple vulnerabilities exist: a vulnerability exist in the 'advSearch_h.asp' script due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists in the 'Custva.asp' script due to insufficient verification of the 'redirectUrl' parameter, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because the software uses a stream encryption algorithm to encrypt passwords in the database using a single key, which could let a local/remote malicious user obtain sensitive information.	Patch available at: <a href="http://www.earlyimpact.com/productcart/support/updates/ProductCart_Security_Update_013004.zip">http://www.earlyimpact.com/productcart/support/updates/ProductCart_Security_Update_013004.zip</a>	ProductCart Multiple Vulnerabilities	<b>Medium/High</b>  <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Exploits have been published.
Ecommerce Corporation <sup>22</sup>	Windows, Unix	Online Store Kit 3.0 Standard, 3.0 Pro, 3.0 Lite	Multiple vulnerabilities exist: a vulnerability exists in the 'more.php' script due to insufficient validation of user-supplied input in the 'id' variable, which could let a remote malicious user execute arbitrary code; and a vulnerability exists because a remote malicious user can create a specially crafted URL that when loaded by a target user, will cause arbitrary scripting code to be executed.	No workaround or patch available at time of publishing.	Online Store Kit Multiple Vulnerabilities	<b>High</b>	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Eggheads Development Team <sup>23</sup>	Unix	Eggdrop IRC bot 1.6.10-1.6.15	A vulnerability exists in the 'Share.mod' component due to a failure to implement intended program logic, which could let a remote malicious user obtain control of an Eggdrop botnet.	The vendor has issued a fix, available via CVS at: <a href="http://www.eggheads.org/cgi-bin/viewcvs.cgi/">http://www.eggheads.org/cgi-bin/viewcvs.cgi/</a>	Eggdrop 'Share Mod' Remote Sharebot Status	<b>High</b>	Bug discussed in newsgroups and websites.

<sup>20</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:011, February 11, 2004.

<sup>21</sup> S-Quadra Security Research Advisory, February 16, 2004.

<sup>22</sup> SystemSecure.org Advisory, February 17, 2004.

<sup>23</sup> SecurityTracker Alert, 1009005, February 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Evolution X <sup>24</sup>	Multiple	Evolution X Build 3935, 3921	Multiple buffer overflow vulnerabilities exist in the FTP server: a vulnerability exists in the 'cd' command after authentication due to insufficient bounds checking, which could let a remote malicious user cause a Denial of Service; a vulnerability exists before authentication when excessive data is submitted as the 'username:password' combination, which could let a remote malicious user cause a Denial of Service; and a vulnerability exists in the 'dir' command when handling excessive data, which could let a remote malicious user cause a Denial of Service. These vulnerabilities could also possibly let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	EvolutionX Multiple Remote Buffer Overflow	Low/High <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
Francisco Burzi <sup>25</sup>	Windows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 BETA 1, FINAL, 6.6, 6.7, 6.9, 7.0, 7.0 FINAL, 7.1	Several vulnerabilities exist: a Cross-Site Scripting vulnerability exists in the 'News' module due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-Site Scripting vulnerability exists in the 'Reviews' due to insufficient sanitization, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	PHP-Nuke 'News' & 'Reviews' Modules Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Francisco Burzi <sup>26</sup>	Windows, Unix	PHP-Nuke 6.0, 6.5, RC1-RC3, 6.5 BETA 1, FINAL, 6.6, 6.7, 6.9, 7.0, 7.0 FINAL, 7.1	An input validation vulnerability exists in the 'public_message()' function due to insufficient sanitization of user-defined parameters, which could let a malicious user execute arbitrary SQL commands.	No workaround or patch available at time of publishing.	PHP-Nuke 'public_message()' Input Validation	High	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

<sup>24</sup> Bugtraq, February 10, 2004.

<sup>25</sup> waraxe-2004-SA#002 Advisory, February 8, 2004.

<sup>26</sup> waraxe-2004-SA#003, February 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Francisco Burzi <sup>27</sup>	Windows, Unix	PHP-Nuke 6.9 & prior	Multiple vulnerabilities exist: a vulnerability exists in the 'index.php' parameter due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; a vulnerability exists in the 'Search' module due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL code; and a vulnerability exists in the 'Web_links' module due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary SQL code.	No workaround or patch available at time of publishing.	PHPNuke Remote SQL Injection	<b>High</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Freeform Interactive <sup>28</sup>	Windows	Purge 1.4.7 & prior, Jihad 2.0.1 & prior	A buffer overflow vulnerability exists due to a boundary error in the client when handling game information received from servers, which could let a remote malicious user execute arbitrary code.	Update available at: <a href="http://www.purgeonline.net/download_2.0.2.shtml">http://www.purgeonline.net/download_2.0.2.shtml</a>	Interactive Purge/Purge Jihad Game Client Remote Buffer Overflow	<b>Low/High</b> <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
GNU <sup>29, 30, 31, 32</sup>	Unix	Mailman 1.0, 1.1, 2.0 beta3 - beta5, 2.0-2.0.13, 2.1, 2.3	A remote Denial of Service vulnerability exists in 'MailCommandHandler.py' when a malicious user submits a specially crafted e-mail message.	Upgrade available at: <a href="http://ftp.gnu.org/gnu/mailman/">http://ftp.gnu.org/gnu/mailman/</a> <b>Debian:</b> <a href="http://security.debian.org/pool/updates/main/m/mailman/">http://security.debian.org/pool/updates/main/m/mailman/</a> <b>Mandrake:</b> <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a> <b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2004-019.html">http://rhn.redhat.com/errata/RHSA-2004-019.html</a> <b>SGI:</b> <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz">ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz</a>	GNU Mailman Remote Denial of Service  <b>CVE Name: CAN-2003-0991</b>	<b>Low</b>	Bug discussed in newsgroups and websites.

<sup>27</sup> SCAN Associates Sdn Bhd Security Advisory, February 10, 2004.

<sup>28</sup> Secunia Advisory, SA10899, February 18, 2004.

<sup>29</sup> Debian Security Advisories, DSA 436-1 & DSA 436-2, February 8 & 21, 2004.

<sup>30</sup> RedHat Security Advisory, RHSA-2004:019-04, February 9, 2004.

<sup>31</sup> SGI Security Advisory, 20040201-01-U, February 11, 2004.

<sup>32</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:013, February 13, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
httpdpalm .source forge.net <sup>33</sup>	PalmOS	Jim Rees httpd for PalmOS; shaun2k2 palmhttpd 3.0	A remote Denial of Service vulnerability exists when a malicious user attempts to establish multiple connections.	Patch available at: <a href="http://www.netwerked.co.uk/code/palmhttpd.patch">http://www.netwerked.co.uk/code/palmhttpd.patch</a> <i>Note: The original "httpd" is no longer maintained.</i>	Palmhttpd Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
IpSwitch <sup>34</sup>	Windows NT 4.0/2000, XP, 2003	IMail 8.0.3, 8.0.5	A buffer overflow vulnerability exists in 'iLDAP.exe' due to a boundary error when handling tags in LDAP messages, which could let a remote malicious user execute arbitrary code.	Hotfix available at: <a href="ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/im805HF2.exe">ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/im805HF2.exe</a>	IMail Server Remote LDAP Daemon Buffer Overflow	High	Bug discussed in newsgroups and websites. Exploit script has been published.
Jelsoft Enter- prises <sup>35</sup>	Windows, Unix	vBulletin 1.0 Lite, 1.1, 1.1.6, 2.0, beta 2&3, 2.0.1, 2.0.2, 2.2.0- 2.2.9 can, 2.3, 2.3.3, 2.3.4	A Cross-Site Scripting vulnerability exists in the 'search.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.	No workaround or patch available at time of publishing.	VBulletin Cross-Site Scripting	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Joe Spanicek <sup>36</sup>	Unix	ShopCart CGI 2.3	A Directory Traversal vulnerability exists because several scripts do not properly validate user-supplied input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	ShopCartCGI Directory Traversal	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
John M Grohol <sup>37</sup>	Unix	Open Journal 2.0-2.0 5	A vulnerability exists in the 'uid' parameter due to an error when handling certain user-supplied input, which could let a remote malicious user bypass authentication and obtain unauthorized access.	Upgrades available at: <a href="http://grohol.com/downloads/oj/latest/oj.tar.gz">http://grohol.com/downloads/oj/latest/oj.tar.gz</a>	OpenJournal Authentication Bypassing	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however exploit information has been published.

<sup>33</sup> Bugtraq, February 8, 2004.

<sup>34</sup> iDEFENSE Security Advisory, February 17, 2004.

<sup>35</sup> Bugtraq, February 12, 2004.

<sup>36</sup> Zone-h Security Team Security Advisory, ZH2004-06SA, February 17, 2004.

<sup>37</sup> SecurityFocus, February 6, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
KarjaSoft <sup>38</sup>	Windows	Sami FTP Server 1.1.3	Multiple remote Denial of Service vulnerabilities exist when processing various commands, including 'CD' and 'GET.'	No workaround or patch available at time of publishing.	Sami FTP Server Multiple Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
KarjaSoft <sup>39</sup>	Windows	Sami HTTP Server 1.0.4	A buffer overflow vulnerability exists when handling 'GET' requests due to insufficient bounds checking, which could let a malicious user cause a Denial of Service or execute arbitrary code.	No workaround or patch available at time of publishing.	Sami HTTP Server GET Request Buffer Overflow	Low/High <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
Konrad Mitchell Lawson <sup>40</sup>	Windows, Unix	Owl's Workshop 1.0	A vulnerability exists in several scripts due to insufficient verification of file and path names, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Owl's Workshop Multiple Remote Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Lavtech. Com Corporation <sup>41</sup>	Windows, Unix	MnoGo Search 3.1.19, 3.1.20, 3.2.10, 3.2.13-3.2.15	A buffer overflow vulnerability exists in the 'UdmDocToText Buf ()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	mnoGoSearch 'UdmDocToTextBuf()' Buffer Overflow	High	Bug discussed in newsgroups and websites.
Linksys <sup>42</sup>	Multiple	WAP55AG 1.0.7	A vulnerability exists in SNMP MIG (Management Information Base) community strings due to an insecure default configuration, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	WAP55AG SNMP Community String Insecure Configuration	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Linux kernel <sup>43</sup>	Unix	Linux kernel 2.6, test9-CVS, test1-test11, 2.6.1 rc1 & rc2	A vulnerability exists because Samba 3.0 combined with Linux Kernel 2.6 fails to strip setuid bits from network shares due to insufficient sanity checks when executing a file that is hosted on a remote Samba share, which could let a remote malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Linux Kernel Samba Share Local Privilege Elevation	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>38</sup> Bugtraq, February 13, 2004.

<sup>39</sup> SP Research Labs Advisory x10, February 17, 2004.

<sup>40</sup> Zone-h Security Team Advisory, ZH2004-08SA, February 18, 2004.

<sup>41</sup> Bugtraq, February 15, 2004.

<sup>42</sup> Bugtraq, February 17, 2004.

<sup>43</sup> Bugtraq, February 9, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
linux-vserver.org <sup>44</sup>	Unix	Linux-VServer 1.20-1.24	A vulnerability exists because the 'chmod()' function does not properly enforce the chmod 000 restriction for vserver directories, which could let a malicious user obtain access to the file system outside of the chrooted root directory.	Patches available at: <a href="http://www.13thfloor.at/vserver/s_release/v1.26/">http://www.13thfloor.at/vserver/s_release/v1.26/</a>	VServer Virtual Server chroot()	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
Macallan Mail Solution <sup>45</sup>	Windows 2000, XP	Macallan Mail Solution 2.8.4.6 (Build 260)	A vulnerability exists when a specially crafted HTTP GET request is submitted for the administration page, which could let a remote malicious user bypass the authentication mechanism.	No workaround or patch available at time of publishing.	Macallan Mail Solution Authentication Bypass	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
MaxWeb Portal.com <sup>46</sup>	Windows, Unix	MaxWeb Portal 1.30, 1.31	Multiple vulnerabilities exist due to insufficient sanitization of user-supplied input: input validation vulnerabilities exist in 'dl_showall.asp' of the 'sub_name' parameter and in 'down.asp' of 'Referer:' headers, which could let a remote malicious user execute arbitrary HTML and script code; an input validation vulnerability exists in 'PersonalMessages' of the 'SendTo' parameter, which could let a remote malicious user execute arbitrary SQL code; and an input validation vulnerability exists in the 'register' form, which could let a remote malicious user execute arbitrary HTML and script code.	Upgrade available at: <a href="http://www.maxwebportal.com/maxwebportal.asp">http://www.maxwebportal.com/maxwebportal.asp</a>	MaxWebPortal Multiple Input Validation	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Microsoft <sup>47</sup>	Windows XP	Windows XP Home, SP1	A vulnerability exists in the HCP URI handler, which could let a remote malicious user execute arbitrary commands.	No workaround or patch available at time of publishing.	Windows XP HCP URI Handler	High	Bug discussed in newsgroups and websites. Exploits have been published.
Microsoft <sup>48</sup>	Windows 98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 6.0, SP-1, Outlook 2002 SP1&SP2, 2003	A remote Denial of Service vulnerability exists because for some web servers, two null (%00) characters appended after the host name cause Internet Explorer or Outlook to consume 100% CPU and freeze.	Frequently asked questions regarding this vulnerability and the patch can be found at: <a href="http://www.microsoft.com/technet/treeview/default.aspx?url=/technet/security/bulletin/MS04-004.asp">http://www.microsoft.com/technet/treeview/default.aspx?url=/technet/security/bulletin/MS04-004.asp</a>	Internet Explorer Double-Null Character Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

<sup>44</sup> Bugtraq, February 6, 2004.

<sup>45</sup> Secunia Advisory, SA10861, February 12, 2004.

<sup>46</sup> Securiteam, February 11, 2004.

<sup>47</sup> Bugtraq, February 7, 2004.

<sup>48</sup> ACROS Security Problem Report, 2004-01-20-1, February 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft <sup>49</sup>	Windows 95/98/ME/NT 4.0/2000, XP, 2003	Internet Explorer 5.0.1, SP1-SP4, 5.5, preview, SP1&SP2, 6.0, SP1	A vulnerability exists when handling 'CHM' files, which could let a remote malicious user execute arbitrary code. <i>Note: It has been reported that this vulnerability is actively being exploited as an infection vector for malicious code that has been temporarily dubbed 'Ibiza.'</i>	No workaround or patch available at time of publishing.	Internet Explorer CHM File Processing Remote Arbitrary Code Execution	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published and this issue is known to be exploited in the wild.

---

<sup>49</sup> SecurityFocus, February 12, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft <sup>50</sup>	Windows NT 4.0/2000, XP, 2003	Windows 2000 Advanced Server, SP1-SP3, 2000 Professional, SP1-SP3, 2000 Server, SP1-SP3, Windows NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Windows Server 2003 Data-center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition, Windows XP 64-bit Edition, SP1, XP 64-bit Edition Version 2003, SP1, XP Home, SP1, XP Professional, SP1	A buffer overflow vulnerability exists in the Microsoft ASN.1 Library due to insufficient checking of user-supplied data, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. <i>Note: Abstract Syntax Notation 1 (ASN.1) is a data standard that is used by many applications and devices in the technology industry for allowing the normalization and understanding of data across various platforms.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at: <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-007.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-007.asp</a>	Microsoft ASN.1 Library Buffer Overflow  CVE Name: CAN-2003-0818	High	Bug discussed in newsgroups and websites. Exploit script has been published.  Vulnerability has appeared in the press and other public media.

<sup>50</sup> Microsoft Security Bulletin. MS04-007, February 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft <sup>51</sup>	Windows NT 4.0/2000, 2003	Windows 2000 Advanced Server, SP1-SP4, 2000 Server, SP1-SP4, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6, Server 2003 Data-center Edition, 64-bit, 2003 Enterprise Edition, 64-bit, 2003 Standard Edition, 2003 Web Edition	A buffer overflow vulnerability exists in Windows Internet Naming Service (WINS) due to the method used to validate the length of specially-crafted packets, which could let a remote malicious user cause a Denial of Service and on some Windows platforms execute arbitrary code.	Frequently asked questions regarding this vulnerability and the patch can be found at:  <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-006.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-006.asp</a>	Windows Internet Naming Service (WINS) Buffer Overflow  CVE Name: CAN-2003-0825	Low/High  <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites.
Microsoft <sup>52</sup>	Windows XP, 2003	Windows XP Home, SP1, XP Media Center Edition, XP Professional, SP1	Several vulnerabilities exist in the NtSystemDebugControl() function, which could let a malicious user with 'SeDebugPrivilege' rights execute arbitrary code.	No workaround or patch available at time of publishing.	Windows 'NtSystemDebugControl()' Kernel API Function Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Microsoft <sup>53</sup>	Windows 95/98/NT 4.0/2000, XP, 2003	Internet Explorer 5.0.1, SP1-SP4, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists that may be exploited via the VBScript LoadPicture method, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Internet Explorer LoadPicture File Enumeration	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

<sup>51</sup> Microsoft Security Bulletin MS04-006, February 10, 2004.

<sup>52</sup> Securiteam, February 19, 2004.

<sup>53</sup> SecurityFocus, February 9, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft <sup>54</sup>	MacOS X 10.1.5, 10.2.1 & later	Virtual PC for Mac 6.0, 6.0.1, 6.0.2, 6.1	A vulnerability exists due to the insecure creation of a temporary log file '/tmp/VPCServices_Log' during execution, which could let a malicious user execute arbitrary code with SYSTEM privileges.	Frequently asked questions regarding this vulnerability and the patch can be found at:  <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-005.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-005.asp</a>	Virtual PC for Mac Temporary File Creation  <b>CVE Name: CAN-2004-0115</b>	<b>High</b>	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft <sup>55</sup>	Windows 95/98/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1&SP2	An integer overflow vulnerability exists caused by a specially crafted bitmap file, which could let a remote malicious user execute arbitrary code. <b>Note: The author states that this flaw was found by reviewing the recently leaked Microsoft Windows source code.</b>	No workaround or patch available at time of publishing.	Internet Explorer Bitmap Processing Integer Overflow	<b>High</b>	Bug discussed in newsgroups and websites. Denial of Service Proof of Concept exploit has been published.
monkeyd.sourceforge.net <sup>56</sup>	Unix	Monkey HTTP Daemon 0.1.4, 0.4-0.4.2, 0.5-0.5.1, 0.6-0.6.3, 0.7.0-0.7.2, 0.8, 0.8.1	A remote Denial of Service vulnerability exists due to an error in the 'get_real_string()' function.	Upgrade available at:  <a href="http://monkeyd.sourceforge.net/get_monkey.php?ver=11">http://monkeyd.sourceforge.net/get_monkey.php?ver=11</a>	Monkey HTTP Daemon Remote Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.
Multiple Vendors <sup>57</sup>	Unix	Linux kernel 2.4.0, test1-test12, 2.4-2.4.24	A Denial of Service vulnerability exists due to an inability of the 'execve()' system function to handle exceptional conditions.	<b>SuSE:</b>  <a href="ftp://ftp.suse.com/pub/suse/i386/update/">ftp://ftp.suse.com/pub/suse/i386/update/</a>	Linux Kernel 'execve()' Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites.

<sup>54</sup> Microsoft Security Bulletin, MS04-005, February 10, 2004.

<sup>55</sup> SecurityTracker Alert, 1009067, February 15, 2004.

<sup>56</sup> Securiteam, February 16, 2004.

<sup>57</sup> SuSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <sup>58</sup>	Windows NT 4.0/2000, XP, 2003	Adobe Acrobat 5.0, 5.0.5, 6.0; Altova xmlspy Enterprise Edition 2004, R4, Home Edition 2004, R4, Professional Edition 2004, R4; AOL Instant Messenger 5.0.2938, 5.1.3036, 5.2.3292, 5.5.3415 Beta; Intuit Quicken 2003, TurboTax 2003; JASC Software PaintShop Pro 5.0, 5.0 1, 5.0 3, 6.0, 6.0 1, 6.0 2, 7.0, 7.0 1, 7.0 2, 7.0 4, 8.0, 8.0 1, 8.10; Music Match Jukebox 8.0-8.2; Van Dyke Technologies Secure CRT 4.0.1-4.0.5; Yahoo! Messenger 5.5- 5.6	An integer overflow vulnerability exists in the ASN.1 handling library, which could let a remote malicious user execute arbitrary code with SYSTEM privileges. <i>Note: Microsoft Windows software that is vulnerable is listed in the Microsoft ASN.1 Library Buffer Overflow entry.</i>	Frequently asked questions regarding this vulnerability and the patch can be found at:  <a href="http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-007.asp">http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS04-007.asp</a>	Multiple Vendors ASN.1 Library Integer Handling  <b>CVE Name: CAN-2003-0818</b>	<b>High</b>	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.  Vulnerability has appeared in the press and other public media.

<sup>58</sup> eEye Digital Security Advisory, AD20040210-2, February 10, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <sup>59, 60</sup>  <i>More advisories issued<sup>61, 62</sup></i>	Unix	Linux Kernel 2.4.22 & prior	A vulnerability exists due to unspecified errors in the R128 Direct Render Infrastructure, which could let a malicious user obtain elevated privileges.	Update available at: <a href="http://www.kernel.org/RedHat">http://www.kernel.org/RedHat:</a> <a href="ftp://updates.redhat.com/">ftp://updates.redhat.com/</a>  <a href="#">Fedora:</a>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a> <a href="#">SuSE:</a>  <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a>	Linux Kernel R128 Device Driver Privilege Escalation  <b>CVE Name: CVE-2004-0003</b>	<b>Medium</b>	Bug discussed in newsgroups and websites.
Multiple Vendors <sup>63, 64</sup>	Unix	Linux kernel 2.4.0, test1-test12, 2.4-2.4.24	A vulnerability exists because the Vicam USB driver does not use the copy_from_user() function to access userspace, which could let a local process cross security boundaries..	Upgrade available at:  <a href="http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.25.tar.bz2">http://www.kernel.org/pub/linux/kernel/v2.4/linux-2.4.25.tar.bz2</a> <b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/">ftp://updates.redhat.com/9/en/os/</a> <b>SuSE:</b> <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a>	Linux Kernel Vicam USB Driver  <b>CVE Name: CAN-2004-0075</b>	<b>Medium</b>	Bug discussed in newsgroups and websites.
Multiple Vendors <sup>65, 66, 67</sup>	Windows, Unix	Metamail 2.7 & prior; RedHat Advanced Workstation for the Itanium Processor 2.1, Enterprise Linux WS 2.1, ES 2.1, AS 2.1	Multiple vulnerabilities exist: a format string vulnerability exists in the 'SaveSquirrel File()' function, which could let a remote malicious user execute arbitrary code; a format string vulnerability exists in the 'PrintHeader()' function, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the 'PrintHeader()' function, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'splitmail' application in the 'ShareThisHeader()' function, which could let a remote malicious user execute arbitrary code.	<b>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/advisories/">http://www.mandrakesecure.net/en/advisories/</a> <b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2004-073.html">http://rhn.redhat.com/errata/RHSA-2004-073.html</a> <b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/slackware-8.1/patches/packages/metamail-2.7-i386-2.tgz">ftp://ftp.slackware.com/pub/slackware/slackware-8.1/patches/packages/metamail-2.7-i386-2.tgz</a>	Metamail Multiple Buffer Overflow & Format String Vulnerabilities  <b>CVE Names: CAN-2004-0104, CAN-2004-0105</b>	<b>High</b>	Bug discussed in newsgroups and websites. Proof of Concept exploits have been published.

<sup>59</sup> Secunia Advisory, SA10782, February 3, 2004.

<sup>60</sup> RedHat Security Advisory, RHSA-2004:044-01, February 3, 2004.

<sup>61</sup> Fedora Security Update Notification, FEDORA-2004-063, February 11, 2004.

<sup>62</sup> SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.

<sup>63</sup> SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.

<sup>64</sup> Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.

<sup>65</sup> Slackware Security Advisory, SSA:2004-049-02, February 18, 2004.

<sup>66</sup> RedHat Security Advisory, RHSA-2004:073-07, February 18, 2004.

<sup>67</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:014, February 19, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
<p>Multiple Vendors 68, 69, 70, 71</p> <p><i>Vendors issue advisories</i> 72, 73</p>	Multiple	Voice over Internet Protocol (VoIP) devices & software; Video conferencing equipment & software; Session Initiation Protocol (SIP) devices & software; Media Gateway Control Protocol (MGCP) devices & software; other networking equipment that may process H.323 traffic (e.g., routers and firewalls)	Various vulnerabilities exist in multiple implementations of the H.323 protocol ranging from a Denial of Service to potential arbitrary code execution.	<p>For workaround and update information see:</p> <p><a href="http://www.uniras.gov.uk/vuls/2004/006489/h323.htm">http://www.uniras.gov.uk/vuls/2004/006489/h323.htm</a></p> <p><u>Debian:</u></p> <p><a href="http://security.debian.org/pool/updates/main/p/pwlib">http://security.debian.org/pool/updates/main/p/pwlib</a></p> <p><u>RedHat:</u></p> <p><a href="ftp://updates.redhat.com/9/en/os/i386">ftp://updates.redhat.com/9/en/os/i386</a></p>	<p>Multiple Vendor H.323 Protocol Implementation Vulnerabilities</p> <p><b>CVE Name: CAN-2003-0819</b></p>	<p><b>Low/High</b></p> <p><b>(Low if a DoS; High if arbitrary code can be executed)</b></p>	Bug discussed in newsgroups and websites.

<sup>68</sup> NISCC Vulnerability Advisory, 006489/H323, January 13, 2004.

<sup>69</sup> Cisco Security Advisory, 47843, January 13, 2004.

<sup>70</sup> CERT® Advisory, CA-2004-01, January 13, 2004.

<sup>71</sup> Sun(sm) Alert Notification, 57476, January 15, 2004.

<sup>72</sup> Red Hat Security Advisory, RHSA-2004:048-01, February 13, 2004.

<sup>73</sup> Debian Security Advisory, DSA 448-1, February 23, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <sup>74, 75, 76, 77</sup>	Unix	Linux kernel 2.4.0, test1-test12, 2.4-2.4.24	A vulnerability exists in the 'ncp_lookup()' function due to insufficient validation of name component lengths, which could let a malicious user execute arbitrary code.	<p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/8/RPMS/">ftp://atualizacoes.conectiva.com.br/8/RPMS/</a></p> <p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a></p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/">ftp://updates.redhat.com/9/en/os/</a></p> <p><b>SuSE:</b>  <a href="ftp://ftp.suse.com/pub/suse/i">ftp://ftp.suse.com/pub/suse/i</a></p>	Linux Kernel NCPFS ncp_lookup() Arbitrary Code Execution  <b>CVE Name:</b> <b>CAN-2004-0010</b>	<b>High</b>	Bug discussed in newsgroups and websites.
Multiple Vendors <sup>78, 79, 80, 81, 82</sup>  <i>More advisories issued</i> <sup>83, 84, 85</sup>	Unix	Gaim version 0.75 & prior	Multiple buffer overflow vulnerabilities exist due to boundary errors in the YMSG protocol handler, the oscar protocol handler, various utility functions, and the HTTP proxy connection handling, which could let a remote malicious user execute arbitrary code.	<p><b>Upgrade available at:</b>  <a href="http://prdownloads.sourceforge.net/ultramagnetic/ultramagnetic-0.81.tar.bz2?download">http://prdownloads.sourceforge.net/ultramagnetic/ultramagnetic-0.81.tar.bz2?download</a></p> <p><b>Debian:</b>  <a href="http://security.debian.org/pool/updates/main/g/gaim/">http://security.debian.org/pool/updates/main/g/gaim/</a></p> <p><b>Mandrake:</b>  <a href="http://www.mandrakesecurity.net/en/advisories/">http://www.mandrakesecurity.net/en/advisories/</a></p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/">ftp://updates.redhat.com/</a></p> <p><b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><b>SuSE:</b>  <a href="ftp://ftp.suse.com/pub/suse/i386/update/">ftp://ftp.suse.com/pub/suse/i386/update/</a></p> <p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a></p> <p><b>SGL:</b>  <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/">ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/</a></p>	Gaim Multiple Remote Buffer Overflow Vulnerabilities  <b>CVE Names:</b> <b>CAN-2004-0005,</b> <b>CAN-2004-0006,</b> <b>CAN-2004-0007,</b> <b>CAN-2004-0008</b>	<b>High</b>	Bug discussed in newsgroups and websites.

<sup>74</sup> Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.

<sup>75</sup> Fedora Security Update Notification, FEDORA-2004-079, February 18, 2004.

<sup>76</sup> SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.

<sup>77</sup> Conectiva Linux Security Announcement, CLA-2004:820, February 20, 2004.

<sup>78</sup> Red Hat Security Advisory, RHSA-2004:032-01, January 26, 2004.

<sup>79</sup> Slackware Security Advisory, SSA:2004-026-01, January 27, 2004.

<sup>80</sup> SuSE Security Announcement, SuSE-SA:2004:004, January 29, 2004.

<sup>81</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:006-1, January 30, 2004

<sup>82</sup> Debian Security Advisory, DSA 434-1, February 5, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <sup>86, 87, 88, 89, 90, 91, 92</sup>	Unix	OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1-12, 4.1-11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3	A buffer overflow vulnerability exists in 'encparse.c' and 'fontfile.c' due to the way font file paths are processed, which could let a malicious user obtain ROOT privileges.	<p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a></p> <p><b>Immunix:</b>  <a href="http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/">http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/</a></p> <p><b>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/advisories/">http://www.mandrakesecure.net/en/advisories/</a></p> <p><b>OpenBSD:</b>  <a href="ftp://ftp.openbsd.org/pub/OpenBSD/patches/">ftp://ftp.openbsd.org/pub/OpenBSD/patches/</a></p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/">ftp://updates.redhat.com/9/en/os/</a></p> <p><b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><b>TurboLinux:</b>  <a href="ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/">ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/</a></p> <p><b>Xfree86:</b>  <a href="ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff">ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.diff</a></p>	XFree86 Buffer Overflow  <b>CVE Name: CAN-2004-0106</b>	<b>High</b>	Bug discussed in newsgroups and websites.

<sup>83</sup> Conectiva Linux Security Announcement, CLA-2004:813, February 10, 2004.

<sup>84</sup> SGI Security Advisory, 20040201-01-U, February 11, 2004.

<sup>85</sup> Fedora Update Notification, FEDORA-2004-070, February 16, 2004.

<sup>86</sup> iDEFENSE Security Advisory, February 12, 2004.

<sup>87</sup> Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.

<sup>88</sup> Fedora Update Notification, FEDORA-2004-069, February 13, 2004.

<sup>89</sup> Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.

<sup>90</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.

<sup>91</sup> Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.

<sup>92</sup> TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors <sup>93, 94, 95, 96, 97, 98, 99</sup>	Unix	OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1-12, 4.1-11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3	A buffer overflow vulnerability exists in the 'font.alias' file due to insufficient validation of user-supplied data, which could let a malicious user obtain ROOT privileges.	<p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a></p> <p><b>Immunix:</b>  <a href="http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/">http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/</a></p> <p><b>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/advisories/">http://www.mandrakesecure.net/en/advisories/</a></p> <p><b>OpenBSD:</b>  <a href="ftp://ftp.openbsd.org/pub/OpenBSD/patches/">ftp://ftp.openbsd.org/pub/OpenBSD/patches/</a></p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/">ftp://updates.redhat.com/9/en/os/</a></p> <p><b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><b>TurboLinux:</b>  <a href="ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/">ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/</a></p> <p><b>Xfree86:</b>  <a href="ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.dif">ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.dif</a></p>	XFree86 Font Information File Buffer Overflow  <b>CVE Name: CAN-2004-0083</b>	<b>High</b>	Bug discussed in newsgroups and websites. Exploit scripts have been published.

<sup>93</sup> iDEFENSE Security Advisory, February 10, 2004.

<sup>94</sup> Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.

<sup>95</sup> Fedora Update Notification, FEDORA-2004-069, February 13, 2004.

<sup>96</sup> Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.

<sup>97</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.

<sup>98</sup> Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.

<sup>99</sup> TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 100, 101, 102, 103, 104, 105, 106	Unix	OpenBSD 3.3, 3.4; XFree86 X11R6 4.1 .0, 4.1-12, 4.1-11, 4.2 .0, 4.2 1, 4.2.1 Errata, 4.3	A buffer overflow vulnerability exists due to insufficient bounds checking when parsing the 'font.alias' file, which could let a remote malicious user execute arbitrary code with ROOT privileges.	<p><b>Fedora:</b> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a></p> <p><b>Immunix:</b> <a href="http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/">http://download.immunix.org/ImmunixOS/7.3/Updates/RPMS/</a></p> <p><b>Mandrake:</b> <a href="http://www.mandrakesecure.net/en/advisories/">http://www.mandrakesecure.net/en/advisories/</a></p> <p><b>OpenBSD:</b> <a href="ftp://ftp.openbsd.org/pub/OpenBSD/patches/">ftp://ftp.openbsd.org/pub/OpenBSD/patches/</a></p> <p><b>RedHat:</b> <a href="ftp://updates.redhat.com/9/en/os/">ftp://updates.redhat.com/9/en/os/</a></p> <p><b>Slackware:</b> <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><b>TurboLinux:</b> <a href="ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/">ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/Desktop/10/updates/</a></p> <p><b>Xfree86:</b> <a href="ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.dif">ftp://ftp.xfree86.org/pub/XFree86/4.3.0/fixes/fontfile.dif</a></p>	Xfree86 Font_Name Buffer Overflow  CAN-2004-0084	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

<sup>100</sup> iDEFENSE Security Advisory, February 12, 2004.

<sup>101</sup> Slackware Security Advisory, SSA:2004-043-02, February 12, 2004.

<sup>102</sup> Fedora Update Notification, FEDORA-2004-069, February 13, 2004.

<sup>103</sup> Immunix Secured OS Security Advisory, IMNX-2004-73-002-01, February 13, 2004.

<sup>104</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:012, February 13, 2004.

<sup>105</sup> Red Hat Security Advisories, RHSA-2004:059-01& RHSA-2004:060-16, February 13, 2004.

<sup>106</sup> TurboLinux Security Advisory, TLSA-2004-5, February 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors 107, 108, 109, 110, 111, 112, 113, 114	Unix	Linux kernel 2.2-2.2.24, 2.4.0, test1-test1 2, 2.4-2.4.24, 2.6. text1-test10, 2.6.1-2.6.2; Netwosix Netwosix Linux 1.0; RedHat kernel-2.4.20-8, athlon.rpm, i386.rpm, i686.rpm, kernel-bigmem-2.4.20-8.i686.rpm, kernel-BOOT-2.4.20-8.i386.rpm, kernel-doc-2.4.20-8.i386.rpm, kernel-smp-2.4.20-8, athlon.rpm, i686.rpm, kernel-source-2.4.20-8.i386.rpm	A vulnerability exists in the 'do_mremap' system function due to insufficient checking of return values, which could let a malicious user execute arbitrary code with ROOT privileges.	Patches available at:  <a href="http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.3.tar.bz2">http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.3.tar.bz2</a>  <a href="http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.3.bz2">http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.3.bz2</a> <b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/8/RPMS/">ftp://atualizacoes.conectiva.com.br/8/RPMS/</a> <b>Debian:</b>  <a href="http://security.debian.org/pool/updates/main/k/kernel-source-2.4.18/">http://security.debian.org/pool/updates/main/k/kernel-source-2.4.18/</a> <b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a> <b>RedHat:</b> <a href="ftp://updates.redhat.com/">ftp://updates.redhat.com/</a> <b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/">ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/</a> <b>SuSE:</b>  <a href="ftp://ftp.suse.com/pub/suse/i386/update/8.2/rp">ftp://ftp.suse.com/pub/suse/i386/update/8.2/rp</a> <b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/">ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/</a>	Linux Kernel do_mremap Function  <b>CVE Name:</b> <b>CAN-2004-0077</b>	<b>High</b>	Bug discussed in newsgroups and websites. Proof of Concept exploit script has been published.

<sup>107</sup> Debian Security Advisories DSA 438-1-DSA 442-1, DSA 444-1, February 18-20, 2004.

<sup>108</sup> Fedora Security Update Notifications, FEDORA-2004-079 & 080, February 18 & 19, 2004.

<sup>109</sup> Red Hat Security Advisory, RHSA-2004:065-01, February 18, 2004.

<sup>110</sup> Slackware Security Advisory, SSA:2004-049-01, February 18, 2004.

<sup>111</sup> SUSE Security Announcement, SuSE-SA:2004:005, February 18, 2004.

<sup>112</sup> Trustix Secure Linux Security Advisory, TSLSA-2004-0007, February 18, 2004.

<sup>113</sup> Netwosix Linux Security Advisory, February 20, 2004

<sup>114</sup> Conectiva Linux Security Announcement, CLA-2004:820, February 20, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Mutt.org <sup>115, 116, 117, 118</sup>	Unix	Mutt 1.2 -1, 1.2.5 .1, 1.2.5 -5, 1.2.5 -4, 1.2.5 - 12OL, 1.2.5 -12, 1.2.5 -1, 1.2.5, 1.3.12 -1, 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	A buffer overflow vulnerability exists when handling some types of e-mail input, which could let a remote malicious user cause a Denial of Service and potentially execute arbitrary code.	Upgrade available at:  <a href="ftp://ftp.mutt.org/pub/mutt/mutt-1.4.2i.tar.gz">ftp://ftp.mutt.org/pub/mutt/mutt-1.4.2i.tar.gz</a> <b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/</a> <b>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a> <b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os">ftp://updates.redhat.com/9/en/os</a> <b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a> <b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/mutt-1.4.2-1tr.i586.rpm">ftp://ftp.trustix.org/pub/trustix/updates/2.0/rpms/mutt-1.4.2-1tr.i586.rpm</a>	Mutt Remote Buffer Overflow  <b>CVE Name: CAN-2004-0078</b>	<b>Low/High</b>  <b>(High if arbitrary code can be executed)</b>	Bug discussed in newsgroups and websites.
Nadeo <sup>119</sup>	Multiple	Track Mania Demo, Virtual Skipper 3	A remote Denial of Service vulnerability exists when a malicious user submits arbitrary data on TCP port 2350.	No workaround or patch available at time of publishing.	Nadeo Game Engine Remote Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. Exploit script has been published.
Nokia <sup>120</sup>	Multiple	Nokia 6310i	Several buffer overflow vulnerabilities exist due to the way the Object Exchange (OBEX) protocol is handled, which could let a remote malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Nokia OBEX Remote Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites.
Opera Software <sup>121</sup>	Windows	Opera Web Browser 7.x	A vulnerability exists when a CLSID is embedded in a file name, which could let a remote malicious user trick a user into opening "trusted" file types which are in fact malicious files.	No workaround or patch available at time of publishing.	Opera Web Browser CLSID File Extension	<b>High</b>	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

<sup>115</sup> Red Hat Security Advisory, RHSA-2004:051-01, February 11, 2004.

<sup>116</sup> Mandrake Linux Security Update Advisory, MDKSA-2004:010, February 11, 2004.

<sup>117</sup> Slackware Security Advisory, SSA:2004-043-01, February 12, 2004.

<sup>118</sup> Trustix Secure Linux Security Advisory, 2004-0006, February 13, 2004.

<sup>119</sup> Bugtraq, February 8, 2004.

<sup>120</sup> Pentest Limited Security Advisory, pfl-2004-01, February 9, 2004.

<sup>121</sup> Secunia Advisory, SA10760, February 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Oracle Corporation <sup>122</sup>  <i>Fix now available</i> <sup>123</sup>	Windows	Oracle HTTP Server (OHS)	A Cross-Site Scripting vulnerability exists in the 'isqlplus' script due to insufficient filtering of user-supplied input in the 'action,' 'username,' and 'password' parameters, which could let a remote malicious user execute arbitrary HTML and script code.	<i>The vendor has made fixes available for customers through the metalink website at: <a href="http://metalink.oracle.com">http://metalink.oracle.com</a></i>	Oracle HTTP Server 'isqlplus' Cross-Site Scripting	<b>High</b>	Bug discussed in newsgroups and websites. Proofs of Concept exploits have been published.
Paul L. Daniels <sup>124</sup>	Unix	Signature DB 0.1.1	A buffer overflow vulnerability exists in the 'sdbscan' program, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SignatureDB 'sdbscan' Buffer Overflow	<b>High</b>	Bug discussed in newsgroups and websites.
Pedro L. Orso <sup>125</sup>	Unix	Mailmgr 1.2.3	A vulnerability exists because temporary files are created in an insecure manner, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Mailmgr Insecure Temporary File Creation	<b>Medium</b>	Bug discussed in newsgroups and websites. There is no exploit code required.
Ratbag <sup>126</sup>	Windows	Dirt Track Racing 1.0 3, 2.0, Dirt Track Racing Australia, Dirt Track Racing Sprint Cars, Leadfoot, World of Outlaws Sprint Cars	A remote Denial of Service vulnerability exists when a malicious user submits a specially crafted packet that specifies a certain number of bytes but does not deliver all of the bytes.	No workaround or patch available at time of publishing.	Ratbag Game Engine Remote Denial of Service	<b>Low</b>	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
RedHat <sup>127</sup>  <i>SGI issues advisory</i> <sup>128</sup>	Unix	Enterprise Linux 2.1AS	A vulnerability exists in the login component of the Util-Linux package due to the way information is handled, which could let a remote malicious user obtain sensitive information.	<b>RedHat:</b> <a href="http://rhn.redhat.com/errata/RHSA-2004-056.html">http://rhn.redhat.com/errata/RHSA-2004-056.html</a>  <b>SGI:</b> <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz">ftp://patches.sgi.com/support/free/security/patches/ProPack/2.3/patch10050.tar.gz</a>	Util-Linux Login Program Information Leakage  <b>CVE Name: CAN-2004-0080</b>	<b>Medium</b>	Bug discussed in newsgroups and websites.

<sup>122</sup> SecurityTracker Alert, 1008838, January 24, 2004.

<sup>123</sup> SecurityFocus, February 6, 2004.

<sup>124</sup> Bugtraq, February 14, 2004.

<sup>125</sup> Bugtraq, February 12, 2004.

<sup>126</sup> SecurityTracker Alert, 1009025, February 12, 2004.

<sup>127</sup> RedHat Security Advisory, RHSA-2004:056-05, February 3, 2004.

<sup>128</sup> SGI Security Advisory, 20040201-01-U, February 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Red-M <sup>129</sup>	Multiple	Red-Alert 3.1	Multiple vulnerabilities exist in various abilities, which could let a remote malicious user cause a Denial of Service, obtain unauthorized access to the administrative interface, or evade detection.	No workaround or patch available at time of publishing.	Multiple Red-Alert Remote Vulnerabilities	Low/ Medium  (Medium if unauthorized access can be obtained or detection evades)	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
RhinoSoft <sup>130</sup>	Windows	Serv-U 4.1 .0.11, 4.1	A buffer overflow vulnerability exists in the 'SITE CHMOD' command when a malicious user file name 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.	Serv-U FTP Server SITE CHMOD Buffer Overflow	Low/High  (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
robotftp.com <sup>131</sup>	Windows	RobotFTP Server 1.0, 2.0 Beta 1	A vulnerability exists when processing 'USER' command arguments of excessive length due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	RobotFTP Server Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept Denial of Service exploit script has been published.
Samba.org <sup>132</sup>	Unix	Samba 3.0, alpha, 3.0.1	A vulnerability exists in the 'mksmbpasswd.sh' shell script, which could let a malicious user obtain unauthorized access.	Upgrade available at: <a href="http://samba.org/samba/whatsnew/samba-3.0.2.html">http://samba.org/samba/whatsnew/samba-3.0.2.html</a> <b>Fedora:</b> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/i386/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/1/i386/</a>	Samba 'Mksmbpasswd.sh' Unauthorized Access  CVE Name: CAN-2004-0082	Medium	Bug discussed in newsgroups and websites. There is no exploit code required; however, an exploit script has been published.
Sambar Technologies <sup>133</sup>	Windows, Unix	Sambar Server 6.0, Beta3	A buffer overflow vulnerability exists in the POST data processing due to a boundary condition error, 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.	Sambar Server Results.STM Post Request Buffer Overflow	Low/High  (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. Exploit script has been published.

<sup>129</sup> Securiteam, February 12, 2004.

<sup>130</sup> Vuln-Dev, February 16, 2004.

<sup>131</sup> Securiteam, February 17, 2004.

<sup>132</sup> Fedora Update Notification, FEDORA-2004-074, February 16, 2004.

<sup>133</sup> SecurityTracker Alert, 1008979, February 8, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Sand Surfer <sup>134</sup>	Unix	Sand Surfer 1.6.5	A user authentication vulnerability exists, which could let a remote malicious user obtain unauthorized access.	Upgrade available at: <a href="http://sourceforge.net/projects/showfiles.php?group_id=31456&amp;package_id=23485">http://sourceforge.net/projects/showfiles.php?group_id=31456&amp;package_id=23485</a>	SandSurfer User Authentication	Medium	Bug discussed in newsgroups and websites.
smallftpd <sup>135</sup>	Windows	smallftpd 1.0.3	A remote Denial of Service vulnerability exists due to a failure to handle multiple connections when performing RETR commands that contain more than 463 slashes ("/").	No workaround or patch available at time of publishing.	SmallFTPD Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Sophos <sup>136</sup>	Windows NT 4.0/2000, XP, 2003, Unix	Anti-Virus 3.4.6, 3.78	Several vulnerabilities exist: a remote Denial of Service vulnerability exists when a malicious MIME header is encountered; and a vulnerability exists when certain types of Delivery Status Notification (DSN) are encountered, which could result in a false sense of security and malicious code completely bypassing detection.	Upgrades available at: <a href="http://www.sophos.com/misc/an">http://www.sophos.com/misc/an</a>	Anti-Virus Remote Denial of Service & Scanner Bypass	Low/High <b>(High if malicious code can be executed)</b>	Bug discussed in newsgroups and websites.
Symantec <sup>137</sup>	Unix	AntiVirus Scan Engine for Red Hat Linux 4.0, 4.3	Multiple vulnerabilities exist due to insecure creation of temporary files during installation, which could let a malicious user corrupt files, cause a Denial of Service or a loss of data.	No workaround or patch available at time of publishing.	AntiVirus Scan Engine For Red Hat Linux Insecure Temporary File	Low/Medium <b>(Low if a DoS)</b>	Bug discussed in newsgroups and websites. There is no exploit code required.
thePalace.com <sup>138</sup>	Windows	The Palace Client 3.5 & prior	A buffer overflow vulnerability exists when processing excessively long links, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	The Palace Graphical Chat Client Remote Buffer Overflow	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
TranSoft Ltd. <sup>139</sup>	Windows	Broker FTP Server 6.1 .0.0	Remote Denial of Service vulnerabilities exist in the 'TsFtpSrv.exe' program.	No workaround or patch available at time of publishing.	Broker FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit has been published.

<sup>134</sup> Secunia Advisory, SA10829, February 12, 2004.

<sup>135</sup> Bugtraq, February 17, 2004.

<sup>136</sup> Sophos Advisory, February 12, 2004.

<sup>137</sup> Secunia Advisory, SA10900, February 17, 2004.

<sup>138</sup> Bugtraq, February 7, 2004.

<sup>139</sup> Securiteam, February 11, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Visual Shapers <sup>140</sup>	Windows, Unix	EzContents 2.0.2 & prior	Several vulnerabilities exist: input validation vulnerabilities exist in the 'modules.php,' 'db.php,' and 'archivednews.php' scripts, which could let a remote malicious user execute arbitrary code; and vulnerability exists in the login, which could let a remote malicious user obtain unauthorized access.	Upgrades available at: <a href="http://www.ezcontentsdev.org/ezContents203.tar.gz">http://www.ezcontentsdev.org/ezContents203.tar.gz</a>	ezContents Multiple Module File Include  CVE Name: CAN-2004-0132	Medium/High  (High if arbitrary code can be executed)	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Vizer Web Server <sup>141</sup>	Windows	Vizer Web Server 1.9.1	A remote Denial of Service vulnerability exists due to insufficient validation of user-supplied input.	No workaround or patch available at time of publishing.	Vizer Web Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
Voice Of Web <sup>142</sup>	Multiple	AllMy Guests 0.1.2, 0.3, 0.4, 0.4.1, AllMy Links 0.3, 0.4, 0.4.1, 0.4.3, 0.4.4, 0.4.9, 0.5, AllMy Visitors 0.3, 0.4	A vulnerability exists in the 'require_once()' call due to insufficient filtering of URI variables, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	AllMyPHP Remote Code Execution	High	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

<sup>140</sup> Bugtraq, February 10, 2004.

<sup>141</sup> SecurityFocus, February 17, 2004.

<sup>142</sup> Bugtraq, February 14, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Web Cortex <sup>143</sup>	Windows	Web Stores 2000	Multiple vulnerabilities exist: a vulnerability exists in 'browse_items.asp' because user input passed to the 'SEARCH_SKU' parameter isn't properly verified, which could let remote malicious user execute arbitrary code; and a vulnerability exists in 'error.asp' because input passed to the 'Message_id' parameter isn't properly verified, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WebStores 2000 Input Validation Vulnerabilities	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Whorl Limited <sup>144</sup>	Windows, Unix	E-Commerce J-Shop Professional v3, JShop Server	A Cross-Site Scripting vulnerability exists in the 'search.php' script due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML or script code.	No workaround or patch available at time of publishing.	JShop E-Commerce Suite xSearch Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
XLIGHT FTP Server <sup>145</sup>	Windows	XLIGHT FTP Server 1.52	A remote Denial of Service vulnerability exists when the 'enable log to screen' option is enabled.	No workaround or patch available at time of publishing.	XLIGHT FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
XLIGHT FTP Server <sup>146</sup>	Windows	XLIGHT FTP Server 1.52	A remote Denial of Service vulnerability exists when a malicious user submits an 'FTP RETR' command with a parameter of more than 260 characters.	No workaround or patch available at time of publishing.	XLIGHT FTP Server Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.
YaBB.org <sup>147</sup>	Windows, Unix	YaBB 1 Gold - SP 1.3.1	An information disclosure vulnerability exists when a login failure occurs, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	YaBB Information Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

<sup>143</sup> S-Quadra Advisory #2004-02-18, February 18, 2004.

<sup>144</sup> SystemSecure.org Advisory, February 7, 2004.

<sup>145</sup> SecurityTracker Alert, 1008965, February 6, 2004.

<sup>146</sup> SecurityFocus, February 16, 2004.

<sup>147</sup> Bugtraq, February 17, 2004.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
YaBB.org <sup>148</sup>	Windows, Unix	YaBB SE 1.5.4, 1.5.5	A vulnerability exists in the in the 'post.php' file due to insufficient verification of the 'quote' parameter, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	YABB SE 'post.php' Arbitrary Code Execution	<b>High</b>	Bug discussed in newsgroups and websites. There is no exploit code required; however, a Proof of Concept exploit has been published.

\*"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 26 and February 18, 2004, 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 45 scripts, programs, and net-news messages containing holes or exploits were identified by US-CERT. *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
February 18, 2004	mremap_poc_2.c	Script that exploits the Linux Kernel do_mremap Function Elevated Privileges vulnerability.
February 18, 2004	purge-cbof.rar	Script that exploits the Interactive Purge/Purge Jihad Game Client Remote Denial of Service vulnerability.
February 18, 2004	testmail1	Proof of Concept exploit for the Metamail Multiple Buffer Overflow & Format String Vulnerabilities.

<sup>148</sup> Bugtraq, February 16, 2004.

Date of Script (Reverse Chronological Order)	Script name	Script Description
February 18, 2004	testmail2	Proof of Concept exploit for the Metamail Multiple Buffer Overflow & Format String Vulnerabilities.
February 18, 2004	testmail3	Proof of Concept exploit for the Metamail Multiple Buffer Overflow & Format String Vulnerabilities.
February 18, 2004	testmail4.splitmail	Proof of Concept exploit for the Metamail Multiple Buffer Overflow & Format String Vulnerabilities.
<b>February 18, 2004</b>	<b>xploit_dbg.cpp</b>	<b>Exploit for the Windows 'NtSystem DebugControl()' Kernel API Function Vulnerabilities.</b>
February 17, 2004	imailRemoteExploit.c	Script that exploits the IMail Server Remote LDAP Daemon Buffer Overflow vulnerability.
<b>February 17, 2004</b>	<b>RobotFTP-dos.c</b>	<b>Script that exploits the RobotFTP Server Remote Denial of Service vulnerability.</b>
<b>February 17, 2004</b>	<b>sp-samihttpddos.c</b>	<b>Script that exploits the Sami HTTP Server GET Request Denial of Service vulnerability.</b>
February 16, 2004	bypassEPA.pdf	Article that discusses how to bypass the Execution Path Analysis used by the PatchFinder utility, avoiding Windows 2k/XP rootkit detection.
February 16, 2004	Monkeydos.rar	Exploit for the Monkey HTTP Daemon Remote Denial of Service vulnerability.
February 16, 2004	nast-0.2.0.tgz	A packet sniffer and a LAN analyzer based on Libnet and Libpcap that can sniff the packets on a network interface in normal mode or in promiscuous mode.
February 16, 2004	Tepick	A textmode sniffer that can track TCP streams and can store all connections in different files or it can display all the stream on the terminal. A useful tool for picking files in a passive way.
February 14, 2004	Asp-POC.pl	Perl script that exploits the ASP Portal Cookie Account Hijack vulnerability.
February 14, 2004	promisc20030313.tar.gz	A sniffer that is based on the AF_PACKET domain socket. It parses the IP, TCP, UDP, ICMP, and ARP protocols.
February 14, 2004	sambascan2-0.3.4.tar.gz	Sambascan2 allows you to search an entire network or a number of hosts for SMB shares and will also list the contents of all public shares that it finds.
February 13, 2004	ASPportal.txt	An exploit for the ASP Portal Cookie Account Hijack vulnerability.
<b>February 12, 2004</b>	<b>crobConDisconExploit.c</b>	<b>Script that exploits the Crob FTP Server Remote Denial of Service vulnerability.</b>
February 11, 2004	X11.fontalias.c	Script that exploits the XFree86 Font Information File Buffer Overflow vulnerability.
<b>February 10, 2004</b>	<b>evoX-dos.pl</b>	<b>Perl script that exploits the EvolutionX Denial of Service vulnerability.</b>
February 10, 2004	MS04-007-dos.c	Script that exploits the Windows ASN.1 Library Integer Handling vulnerability.
<b>February 10, 2004</b>	<b>phpNukeSearchModExploit.php</b>	<b>Exploit for the PHPNuke Remote SQL Injection vulnerability.</b>
<b>February 10, 2004</b>	<b>The_First_Cut_Is_The_Deeppest.txt</b>	<b>An exploit for PHPNuke versions 6.x and greater that extracts the administrator hash using a SQL injection attack.</b>
February 10, 2004	xFreeFontBufO.c	Script that exploits the XFree86 Font Information File Buffer Overflow vulnerability.
February 9, 2004	kismet-feb.04.01.tar.gz	A 802.11 layer 2 wireless network sniffer that can sniff 802.11b, 802.11a, and 802.11g traffic. It is capable of sniffing using almost any wireless card supported in Linux, which currently divide into cards handled by libpcap and the Linux-Wireless extensions (such as Cisco Aironet), and cards supported by the Wlan-NG project which use the Prism/2 chipset (such as Linksys, Dlink, and Zoom).

Date of Script (Reverse Chronological Order)	Script name	Script Description
February 8, 2004	palmhttpd_dos.c	Exploit for the Palmhttpd Server Remote Denial of Service vulnerability.
February 8, 2004	PalmOShttpd.txt	Exploit for the Palmhttpd Server Remote Denial of Service vulnerability.
<b>February 8, 2004</b>	<b>phpNukeSQLinj.pl</b>	<b>Perl script that exploit the PHP-Nuke 'public_message()' Input Validation vulnerability.</b>
<b>February 8, 2004</b>	<b>sambarSmudge.py</b>	<b>Script that exploits the Sambar Server Results.STM Post Request Buffer Overflow vulnerability.</b>
<b>February 8, 2004</b>	<b>trackmania_dos.c</b>	<b>Script that exploits the Nadeo Game Engine Remote Denial of Service vulnerability.</b>
February 6, 2004	chrootAgainExploit.c	Script that exploits the VServer Virtual Server chroot() vulnerability.
<b>February 6, 2004</b>	<b>dreamFTPNightmare.c</b>	<b>Script that exploits the BolinTech Dream FTP Server User Name Format String vulnerability.</b>
February 6, 2004	systemsearcher.tgz	A Linux security scanner written in Perl that scans single hosts or subnets for anonymous FTP servers, TFTP servers, SMTP servers which allow relaying, SSH servers, Telnet servers, NFS servers with exported directories, mail servers, Web servers (HTTP/HTTPS), well-known Trojan ports, and exploitable CGIs.
February 5, 2004	vserver_chroot.txt	Local exploit for the VServer Virtual Server chroot() vulnerability.
February 3, 2004	chaser-adv.txt	Exploit for the Chaser memory allocation vulnerability.
February 3, 2004	chaser-client.zip	Test exploit for the server of Chaser versions 1.50 and below memory allocation vulnerability.
February 3, 2004	chasercrash.zip	Test exploit for the server of Chaser versions 1.50 and below memory allocation vulnerability.
February 2, 2004	ADMsb_0.3.tar.gz	A security scanner for Samba based on the source of smbclient. That will get the netbios name, share list, workgroup, domain, and OS.
<b>February 2, 2004</b>	<b>overkill.txt</b>	<b>Exploit for the Overkill Game Client Multiple Buffer Overflows vulnerabilities.</b>
February 2, 2004	tcpick-0.1.20.tar.gz	A textmode sniffer that can track TCP streams and saves the data captured in files or displays them in the terminal.
February 2, 2004	uniqueid-0.5.0.tar.gz	A Perl CGI that calculates and reverse engineers driver's license numbers.
January 30, 2004	sslexp.c	Brute forcer for OpenSSL ASN.1 parsing vulnerabilities.
January 30, 2004	winblast.sh	Script that exploits the Windows XP/2003 Samba Denial of Service vulnerability.
<b>January 26, 2004</b>	<b>proxyNow2x.txt</b>	<b>Perl script that exploits the ProxyNow Multiple Buffer Overflow vulnerability.</b>

## Trends

- **US-CERT has become aware of publicly available exploit code for the ASN.1 vulnerability. For more information see Microsoft ASN.1 Library Buffer Overflow and Multiple Vendors ASN.1 Library Integer Handling entries in "Bugs, Holes & Patches" Table above.**
- **US-CERT has received reports of a new mass-mailing virus, referred to as "W32/Netsky.B," "WORM\_NETSKY.B," or "Moodown.B." It can spread via e-mail, or network file shares. For more information, see W32/Netsky-B entry (item is boldfaced/red) in the Virus Section below and US-CERT entry located at: <http://www.us-cert.gov/current/>.**
- **US-CERT has received reports of a new mass-emailing virus, referred to as "W32/Bagle.B," "W32/Bagle.B," or "W32.Alua." For more information, see Win32/Bagle.B entry (item is**

**boldfaced/red) in the Virus Section below and US-CERT entry located at: <http://www.us-cert.gov/current/>.**

- **On February 9, 2004, the CERT/CC began receiving reports of a new variant of the Mydoom virus known as W32/Mydoom.C or W32.HLLW.Doomjuice. Systems previously infected with Mydoom.A have a backdoor listening on port 3127/tcp. For more information, see CERT/CC entry located at: <http://www.cert.org/current>.**
- **A new variant of the previously discovered MyDoom virus, MyDoom.B, has been identified. In addition to the common traits of email-borne viruses, this virus may prevent your computer from updating anti-virus and other software. For more information, see Cyber Security Alert, SA04-028A, located at: <http://www.us-cert.gov/cas/alerts/SA04-028A.html>.**
- A Trojan horse program that appears to be a Microsoft Corp. security update can download malicious code from a remote Web site and install a back door on the compromised computer, leaving it vulnerable to remote control.

## 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/MyDoom-A	Worm	New to Table	January 2004
2	W32/Bagle-A	Worm	Stable	January 2004
3	W32/Sober-C	Worm	Increase	December 2003
4	W32/Swen	Worm	Increase	September 2003
5	W32/Netsky.B	Worm	New to Table	February 2004
6	W32/Klez.H	Worm	Decrease	April 2002
7	W32/Bagle-B	Worm	New to Table	February 2004
8	W32/Dumaru-A	Worm	Decrease	August 2003
9	W32/Sobig.F	Worm	Decrease	August 2003
10	W32/Mimail-A	Worm	Decrease	August 2003

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, and The WildList Organization International.

**BAT\_REDWA.A (Batch File):** This mass-mailing batch file spreads via e-mail, Internet Relay Chat (IRC) and peer-to-peer file-sharing applications. However, it fails to execute some of its intended routines due to programming errors. It sends copies of itself with the following details to all e-mail addresses found in the address book of a target user:

- Subject: Symantec Security Alert
- Attachment: Symantec\_W32\_Cure.bat

It also deletes several antivirus programs. It runs on Windows 95, 98, ME, NT, 2000, and XP.

**HTML\_SWENFRAUD.A (HTML Virus):** This HTML malware may arrive as a fake Microsoft security update e-mail or may be visited directly as a web page by unsuspecting users. It uses a known Internet Explorer vulnerability that allows a web page to spoof its URL as displayed on the Internet Explorer address and status bars. It displays a spoofed page to trick users into providing sensitive information. The malware persuades the user to click on a button, which when clicked, points to a malicious web page. HTML\_SWENFRAUD.A also invokes confidence in an unknowing user to enter personal data to a malicious web site. For more information regarding this vulnerability, visit the following Microsoft page:

- Microsoft Security Bulletin 04-004

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

**VBS.Laske@mm (Visual Basic Script Worm):** This is a mass-mailing worm written in Visual Basic (VB) Script. It also attempts to delete all the content from drives A through P.

**VBS/Lucave (Visual Basic Script Worm):** This VBScript virus code contains errors and some payloads will not be executed. The virus code is encrypted and on executing the infected script, the virus will copy itself to the hard coded directory: C:\windows\alias.jpg.vbs. It will also copy itself to random network drives as [random character]alias.jpg.vbs. The virus attempts to copy itself to random IP sites. The following registry key will be added:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ Run  
"Gnsys" = C:\windows\alias.jpg.vbs

VBS/Lucave contains mass mailing capabilities, IRC propagation, and utilizes the Windows Management Instrumentation (WMI), but this is not executed due to the error in the virus code

**VBS\_QOMA.A (Alias: QOMA.A) (Visual Basic Script Worm):** This Visual Basic (VB) script propagates via e-mail with the following details:

- Subject: Heyy..Check this
- Attachment: copy.vbs

It sends copies of itself to all e-mail addresses found in the Microsoft Outlook and also adds several system policies that restrict user access. These restrictions make the cleaning of this malware, particularly the disabled registry tools, more difficult. It runs on Windows 95, 98, ME, NT, 2000, and XP.

**W32/Agobot-CP (Alias: Backdoor.Agobot.3.gen) (Win32 Worm):** This is an IRC backdoor Trojan and network worm. It copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks, please see Microsoft Security Bulletins MS03-001 and MS03-026. MS03-026 has been superseded by Microsoft security bulletin MS03-039. When first run, W32/Agobot-CP copies itself to the Windows system32 folder with the filename winpn32.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\WinPN32= winpn32.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\WinPN32= winpn32.exe

It connects to a remote IRC server and joins a specific channel. The backdoor functionality of the worm can then be accessed by a malicious user using the IRC network. The worm also attempts to terminate and disable various security-related programs.

**W32/Agobot-CW (Alias: Backdoor.Agobot.3.gen) (Win32 Worm):** This is an IRC backdoor Trojan and network worm. It copies itself to network shares with weak passwords and attempts to spread to computers using the DCOM RPC and the RPC locator vulnerabilities. These vulnerabilities allow the worm to execute its code on target computers with System level privileges. For further information on these vulnerabilities and for details on how to protect/patch the computer against such attacks, please see Microsoft Security Bulletins MS03-001 and MS03-026. MS03-026 has been superseded by Microsoft security bulletin MS03-039. When first run, W32/Agobot-CW copies itself to the Windows system32 folder with the filename winpn32.exe and creates the following registry entries so that the worm is run when Windows starts up:

- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\Diagnostic Agent = diagent.exe
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices\Diagnostic Agent = diagent.exe

It connects to a remote IRC server and joins a specific channel. The backdoor functionality of the worm can then be accessed by a malicious user using the IRC network. The worm also attempts to terminate and disable various security-related programs.

**W32/Deadhat-A (Aliases: Win32.Vesser.A, W32.HLLW.Deadhat, Vesser, W32/Vesser.worm.a, Vesser, W32/Deadhat.worm.a, WORM\_DEADHAT.A, Win32.Deadhat.A, Worm.Win32.Vesser) (Win32 Worm):** This is a worm that spreads via the Soulseek file sharing network and computers infected with W32/MyDoom-A worm. If the worm detects that it is being debugged, it does not spread but attempts to delete various system files. In order to run automatically when Windows starts up, the worm copies itself to the file sms.exe in the Windows system folder and adds the registry entry:

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

pointing to the worm binary. When executed, the worm may display a message box: "Error executing program!" It also copies itself to the shared folder of an existing Soulseek installation using various filenames. W32/Deadhat-A attempts to end various security and anti-virus related processes. It listens on TCP port 2766. The port may be used to receive and run file in the temporary folder. W32/Deadhat-A also has an IRC backdoor component. The worm attempts to connect to one of a list of IRC servers and receives commands that allow a remote malicious user control over the infected computer. W32/Deadhat-A scans network address ranges for ports opened by the W32/MyDoom-A. The worm generates IP addresses of the format a.b.c.d where d is taken from an internal list, c is a random number and the values for a and b are enumerated consecutively starting from 0. If an open port is found, W32/Deadhat-A attempts to copy itself to the remote machine.

**W32/Deadhat-B (Aliases: Worm.Win32.Vesser.b, W32.HLLW.Deadhat.B, WORM\_DEADHAT.B) (Win32 Worm):** This worm spreads via the SoulSeek file sharing network and computers infected with the W32/MyDoom worm. It creates a copy of itself in the system folder with the filename msgsrv32.exe and sets the following registry entry so that the worm is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\msgsrv32

The worm copies itself to the shared folder of an existing SoulSeek installation using various filenames. W32/Deadhat-B has a backdoor component listening on TCP port 2766. W32/Deadhat-B also has an IRC backdoor component. The worm attempts to connect to one of a list of IRC servers and receives commands that allow a remote malicious user control over the infected computer via this channel. W32/Deadhat-B scans network address ranges for ports opened by the W32/MyDoom worm and will attempt to copy itself to compromised machines. The worm may attempt to delete various system files. W32/Deadhat-B also attempts to terminate various system monitoring and anti-virus related processes.

**W32.Dinfor.Worm (Alias: WORM\_SDBOT.FP) (Internet Worm):** This is a worm that spreads across network shares. It exploits weak passwords and uses the DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-039) to create user accounts on remote computers. This worm also acts as a backdoor, connecting to an IRC channel and allowing a remote malicious user to control an infected computer.

**W32/DoomHunt-A (Aliases: W32.Doomhunter, W32/Doomhunter.worm, Win32:Doomhunter [Wrm], WORM\_DOOMHUNTR.A) (Win32 Worm):** This is a worm that spreads to computers infected with the W32/MyDoom-A and W32/MyDoom-B worms. It terminates processes and removes files associated with these worms. W32/DoomHunt-A listens for connections on port 3127. If a connection is made, the worm sends back a copy of itself to be executed on the remote computer. When run, the worm copies itself to the Windows system folder using the filename worm.exe and creates the following registry entry to ensure it is run at system logon:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\DELETE ME

W32/DoomHunt-A will end various processes and delete various files.

**W32/Doomjuice-B (Aliases: W32.DoomJuice.B, WORM\_DOOMJUICE.B, Doomjuice.B, W32.HLLW.Doomjuice.B, W32/Doomjuice.worm.b, WORM\_DOOMJUICE.B) (Win32 Worm):** This is a worm that spreads by exploiting a backdoor installed by W32/MyDoom-A. The functionality of the worm is similar to W32/Doomjuice-A but without the part of the code that drops the archive with the W32/MyDoom-A source code. The worm creates a copy of itself named regedit.exe in the Windows system folder and creates the following registry entry to ensure that the copy is run when Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\NeroCheck= <system folder>regedit.exe

W32/Doomjuice-B will contact computers infected with W32/MyDoom-A by attempting to connect to port 3127 of randomly chosen IP addresses. If the worm contacts a computer infected with W32/MyDoom-A, a copy of W32/Doomjuice-B will be transferred to the computer and executed. On 13th February and any date thereafter, the W32/Doomjuice-B will attempt to launch a Denial of Service attack against www.microsoft.com. The DoS attack routine is changed in order to make blocking of the worm HTTP requests difficult.

**W32.Dumaru.AH@mm (Aliases: W32/Mimail.u@MM, Win32.Mimail.U) (Win32 Worm):** This is a multi-threaded, mass-mailing worm that opens a backdoor, runs a keylogger, and attempts to steal personal information. The worm uses its own SMTP engine to spread to e-mail addresses that it finds in the files on an infected system. The e-mail has the following characteristics:

- From: random characters@<a domain from an e-mail addresses found on the infected computer>
- Subject: Unknown
- Attachment: document.zip (The attachment is a zip file that contains the worm executable, myphoto.jpg<56 spaces>.exe.)

The worm is similar to the W32.Dumaru.Y@mm worm and arrives as a dropper.

**W32.HLLW.Antinny.E (Win32 Worm):** This is a variant of W32.HLLW.Antinny. This worm spreads using the Winny file-sharing network.

**W32.HLLW.Cult.M@mm (Win32 Worm):** This is a mass-mailing worm that uses its own SMTP engine to send itself to randomly generated e-mail addresses. The worm also has IRC Trojan functionality that allows the Trojan's creator to control the infected computer by using Internet Relay Chat (IRC). The e-mail message has the following characteristics:

- Subject: Hello , I sent you a beautiful Love Card ^\_\*
- Attachment: LoveCard.pif

This threat is compressed with ASPack.

**W32.HLLW.Moega.AG (Alias: W32.HLLW.Moega.E) (Win23 Worm):** This is a variant of W32.HLLW.Moega.E that has backdoor capabilities. It attempts to spread through the local area network. The worm connects to an IRC server to receive further instructions from a malicious user. The W32.HLLW.Moega.AG executable icon looks similar to that of the Windows XP Windows Update executable, Wupdated.exe.

**W32.HLLP.Shodi (Win32 Virus):** This is a simple virus that prepends itself to files.

**W32.HLLP.Yero.Worm (Win32 Worm):** This is a worm that attempts to copy itself to remote computers. It also has backdoor and file-infecting capabilities. The threat is written in Delphi and is packed with UPX.

**W32/MyDoom-E (Aliases: W32.Mydoom.A@mm, I-Worm.MyDoom.d, W32/Mydoom.e@MM, WORM\_MYDOOM.E) (Win32 Worm):** This is a worm that spreads by e-mail. When the infected attachment is launched, the worm harvests e-mail addresses from address books and from files with the following extensions: wab, htm, txt, sht, php, asp, dbx, tbb, adb, and pl. W32/MyDoom-E uses randomly chosen e-mail addresses in the "To:" and "From:" fields as well as a randomly chosen subject line. The e-mails distributing this worm will have various subject lines and attachment files. Attached files will have an extension of BAT, CMD, EXE, PIF, SCR, or ZIP. The worm will also copy itself into the shared folder of the KaZaA peer-to-peer application with various filenames and a PIF, EXE, SCR or BAT extension. W32/MyDoom-E will copy itself to the Windows system folder using the filename taskmon.exe and sets the following registry entry to point to this copy to ensure it is run at system logon:

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

Please note that on Windows 95/98/ME, there is a legitimate file called taskmon.exe in the Windows folder. W32/MyDoom-E will create the file shimgapi.dll in the Windows system or temp folder. This is a backdoor program loaded by the worm that allows outsiders to connect to TCP port 3127. The DLL adds the following registry entry so that it is run on startup:

- HKCR\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32\Default="<location of dll>"

Between the 1st February 2004 and 14th February 2006, the worm will attempt a Denial of Service attack on www.sco.com. After the 14th February 2006 W32/MyDoom-E will no longer spread; however, it will still run the backdoor component.

**W32/Nachi-B (Aliases: W32/Welchia.B.Worm, Welchi.B, W32/Nachi.B, W32/Nachi.worm.b, WORM\_NACHI.B, W32.Welchia.B.Worm, Win32.Nachi.B, WORM\_NACHI.B, Worm.Win32.Welchia.b) (Win32 Worm):** This is a worm that attempts to remove files associated with the W32/MyDoom-A and W32/MyDoom-B worms. It spreads by exploiting the following Microsoft vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
  - Microsoft issued a patch for the vulnerability exploited by this worm on July 16, 2003. The patch is available from <http://www.microsoft.com/technet/security/bulletin/MS03-026.asp>. MS03-026 has been superseded by Microsoft security bulletin MS03-039.
- WebDAV vulnerability and IIS5/WEBDAV Buffer Overrun vulnerability
  - Microsoft issued a patch for the vulnerability exploited by this worm on March 17, 2003. The patch is available from <http://www.microsoft.com/technet/security/bulletin/MS03-007.asp>.

When run, the worm copies itself to the subfolder drivers located in the Windows system folder using the filename svchost.exe. The worm also tries to download and execute some of the following Microsoft patches:

- <http://download.microsoft.com/download/4/d/3/4d375d48-04c7-411f-959b-3467c5ef1e9a/WindowsXP-KB828035-x86-CHS.exe>
- <http://download.microsoft.com/download/a/4/3/a43ea017-9abd-4d28-a736-2c17dd4d7e59/WindowsXP-KB828035-x86-KOR.exe>
- <http://download.microsoft.com/download/e/a/e/ea4109-0870-4dd3-88e0-a34035dc181a/WindowsXP-KB828035-x86-ENU.exe>
- <http://download.microsoft.com/download/9/c/5/9c579720-63e9-478a-bdcb-70087ccad56c/Windows2000-KB828749-x86-CHS.exe>
- <http://download.microsoft.com/download/0/8/4/084be8b7-e000-4847-979c-c26de0929513/Windows2000-KB828749-x86-KOR.exe>
- <http://download.microsoft.com/download/3/c/6/3c6d56ff-ff8e-4322-84cb-3bf9a915e6d9/Windows2000-KB828749-x86-ENU.exe>

W32/Nachi-B checks every twenty minutes for a live internet connection by attempting to connect to either microsoft.com, intel.com, or google.com and will attempt to infect random IP addresses if the connection was successful. W32/Nachi-B will uninstall itself from June 2004. It may overwrite files with extensions SHTML, SHTM, STM, CGI, PHP, HTML, HTM, and ASP.

**W32/Nachi.worm.c (Aliases: W32.Welchia.C.Worm, WORM\_NACH1.C) (Win32 Worm):** This is a minor variation of, and functionally equivalent to W32.Welchia.B.Worm. If the version of the operating system of the infected machine is Chinese, Korean, or English, the worm will attempt to download the Microsoft Workstation Service Buffer Overrun and Microsoft Messenger Service Buffer Overrun patches from the Microsoft® Windows Update Web site, install it, and then restart the computer. The worm also attempts to remove W32.Mydoom.A@mm and W32.Mydoom.B@mm worms. W32.Welchia.C.Worm exploits multiple vulnerabilities, including:

- The DCOM RPC vulnerability (described in Microsoft Security Bulletin MS03-026) using TCP port 135. The worm specifically targets Windows XP machines using this exploit.
- The WebDav vulnerability (described in Microsoft Security Bulletin MS03-007) using TCP port 80. The worm specifically targets machines running Microsoft IIS 5.0 using this exploit. The worm's use of this exploit will impact Windows 2000 systems and may impact Windows NT/XP systems.
- The Workstation service buffer overrun vulnerability (described in Microsoft Security Bulletin MS03-049) using TCP port 445.
- The Locator service vulnerability using TCP port 445 (described in Microsoft Security Bulletin MS03-001). The worm specifically targets Windows 2000 machines using this exploit.

The presence of the file, %Windir%\system32\drivers\svchost.exe, is an indication of a possible infection. This threat is compressed with UPX.

**W32/Netsky.A, (Aliases: WORM\_NETSKY.A, I-Worm.Moodown, Moodown, W32.Netsky@mm) (Win32 Worm):** This worm spreads via e-mail and peer-to-peer networks. It creates a copy of itself as SERVICES.EXE in the Windows folder and uses an icon similar to that of MS Word. As this malware's stealth mechanism, it displays the following message: "The file could not be opened!" To spread, it sends an e-mail via SMTP (Simple Mail Transfer Protocol). This worm also spreads via peer-to-peer networks. It drops copies of itself in the shared folders of file-sharing applications. It runs on Windows 2000 and XP.

**W32/Netsky-B (Aliases: Win32/Netsky.B, I-Worm.Moodown.B, W32/Netsky.b@MM, Moodown.B, W32.Netsky.B@mm, Win32.Netsky.B, WORM\_NETSKY.B) (Win32 Worm):** This worm has been reported in the wild. It spreads by e-mail and Windows network shares. W32/Netsky-B copies itself into the Windows folder as services.exe. In order to run automatically when Windows starts up W32/Netsky-B creates the following registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\service="C:\\WINDOWS\\services.exe -serv"

W32/Netsky-B searches all mapped drives for files with the following extensions in order to find e-mail addresses: MSG, OFT, SHT, DBX, TBB, ADB, DOC, WAB, ASP, UIN, RTF, VBS, HTML, HTM, PL, PHP, TXT, and EML. It searches drives C: to Z: and attempts to copy itself into folders with names containing the string "share" or "sharing." The worm uses various file names with it copies itself to share folders. It may arrive in an e-mail with the various subject lines, message text, and attachment file names. The extension is combination of DOC, RTF, HTM, PIF, COM, SCR, and EXE. W32/Netsky-B may also send a ZIP file. The e-mail address of the sender will be spoofed. When the attachment is opened, W32/Netsky-B may display a fake message box "The file could not be opened." W32/Netsky-B attempts to remove registry entries related to few recent viruses, including W32/MyDoom-A and W32/MyDoom-B.

**W32.Rusty@m (Aliases: W32.Rusty, Crusty, WORM\_RUSTY.A) (Win32 Worm):** This is an e-mail worm that uses MAPI to spread through Microsoft Outlook. It also copies itself to various instant messenger and file-sharing program folders. The e-mail message has various subject lines and attachments. W32.Rusty@m is written in Visual Basic.

**W32/Wukill-B (Aliases: I-Worm.Rays, Win32/Wukill.B, W32.Wullik.B@mm, WORM\_WUKILL.B) (Win32 Worm):** This is an Internet worm that can e-mail itself to contacts found in the Microsoft Outlook address book. The worm copies itself to the Windows folder as MSTRAY.EXE and creates the following registry entry so that MSTRAY.EXE is run automatically each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\RavTimeXP=  
<WINDOWS>\MSTRAY.EXE

The worm may copy itself to the A: floppy drive as Winkill.exe and may also copy itself to the following folders using random filenames consisting of 1-5 characters B-Z with an extension of EXE:

- <WINDOWS>\System
- <WINDOWS>\Web
- <WINDOWS>\Fonts
- <WINDOWS>\Temp
- <WINDOWS>\Help

W32/Wukill-B may also drop a harmless data file called <WINDOWS>\Winfile.ini and COMMENT.HTT and DESKTOP.INI as hidden, system files in the root folder. This worm may display the message "Warning. This File Has Been Damage!" upon execution. W32/Wukill-B may open the File Manager application when executed on the 28th of the month.

**W32.Yenik.A@mm (Aliases: W32/Yenik.worm, I-Worm.Yenik, W32/Yenik.A.worm) (Win32 Worm):** This is a worm that attempts to e-mail itself to the addresses found in the Windows address book. The e-mail attachment will have a variable subject and variable attachment name. The attachment will have a .exe file extension. It will also attempt to spread through file-sharing programs, such as KaZaA, Morpheus, eMule, eDonkey, BearShare, and Grokster, as well as ICQ. It is written in C and is packed with UPX.

**W97M.Saver.H (Aliases: Macro.Word97.Saver, W97M/Doccopy.A) (Word 97 Macro Virus):** This is a macro virus that infects Microsoft Word documents and templates. It will create a copy of the infected document as "saver.dll."

**Win32/Bagle.B (Aliases: W32/Tanx-A, Bagle.B, W32/Bagle.b@MM, W32.Alua@mm, WORM\_BAGLE.B, Win32.Bagle.B, I-Worm.Bagle.b, Win32:Beagle-B, I-Worm/Bagle.B, Worm/Bagle.B) (Win32 Worm):** This worm has been reported in the wild. It is a worm that uses e-mail to spread. The worm arrives in a message with the following characteristics:

- Subject line: ID <random characters>... thanks
- Attached file: <random\_file\_name>.exe

The address of the sender is spoofed. When the attached infected file is run, it copies itself into the Windows system folder as au.exe and changes creates the following registry entry so that the worm file is run during the Windows startup:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\au.exe = <windows system folder>\au.exe

If the filename of the launched file is not au.exe, the worm attempts to launch the Windows sound recorder application sndrec32.exe. It searches all fixed drives recursively for files with the extension WAB, TXT, HTM, and HTML. These files are searched for e-mail addresses that are later used to fill in the sender and recipient fields of the e-mail message. Win32/Bagle.B opens a TCP port 8866 and listens for connections. The backdoor may be used to update the worm file. It will connect to the following websites and submit information about the listening port and the randomly generated infection ID:

- www.47df.de
- www.strato.de and
- intern.games-ring.de

Win32/Bagle.B uses the registry key HKCU\Software\Windows2000 to store some other data values (like the randomly created infection ID). The registry values used are gid and frn. The worm will stop spreading after 25 February 2004.

**WORM\_AGOBOT.AL (Alias: Backdoor.Agobot3.cs) (Win32 Worm):** This memory-resident malware that has both worm and backdoor capabilities. It exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

For more information about these Windows vulnerabilities, please refer to the following Microsoft Web pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It drops itself as the file EXPLORE.EXE in the Windows system folder. The worm attempts to log into systems using a list of user names and passwords. It opens port 6667 and tries to connect to an Internet Relay Chat (IRC) server and then listens for commands from the bot through an IRC channel. Upon establishing connection, this malware allows a remote user to execute malicious commands on the infected system. It also terminates AntiVirus-related processes and steals CD keys of certain game applications. This malware is compressed using ASPack and UPX. It runs on Windows NT, 2000, and XP.

**WORM\_AGOBOT.CT (Internet Worm):** This worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

For more information about these Windows vulnerabilities, please refer to the following Microsoft Web pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It attempts to log into systems using a list of user names and passwords and then drops a copy. It also terminates AntiVirus-related processes and steals CD keys of certain game applications. It also has backdoor capabilities and may execute remote commands in the host machine. It runs on Windows NT, 2000, and XP.

**WORM\_AGOBOT.CX (Internet Worm):** This worm exploits certain vulnerabilities to propagate across networks. Like the earlier AGOBOT variants, it takes advantage of the following Windows vulnerabilities:

- Remote Procedure Call (RPC) Distributed Component Object Model (DCOM) vulnerability
- IIS5/WEBDAV Buffer Overflow vulnerability
- RPC Locator vulnerability

For more information about these Windows vulnerabilities, please refer to the following Microsoft Web pages:

- Microsoft Security Bulletin MS03-026
- Microsoft Security Bulletin MS03-001
- Microsoft Security Bulletin MS03-007

It runs on Windows NT, 2000, and XP.

**WORM\_DEADHAT.C (Internet Worm):** This memory-resident worm propagates on systems that are infected with WORM\_MYDOOM.A and WORM\_MYDOOM.B. It is also capable of spreading via the popular peer-to-peer file-sharing application, SoulSeek. It has the following capabilities:

- Drop itself as the file LMSS.EXE in the C:\WINNT\System32\folder (Note: This path is hardcoded in the malware code. If this folder does not exist on the system, it fails to drop its copy.)
- Enumerate all running processes
- Terminate processes associated with AntiVirus programs
- Terminate instances of WORM\_MYDOOM.A and WORM\_MYDOOM.B

- Delete several system files such as BOOT.INI and AUTOEXEC.BAT
- Open port 2766, connect to an Internet Relay Chat (IRC) server, and joins a channel to wait for malicious commands from a remote user

It runs on Windows 98, ME, NT, 2000, and XP.

**WORM\_DUMARU.AC (Internet Worm):** This worm has been reported in the wild. It is a polymorphic mass-mailing worm that spreads via e-mail. It drops and executes a copy of itself as NLOAD.EXE in the root directory. It employs several autostart techniques so that it runs at every system startup. It uses SMTP (Simple Mail Transfer Protocol) to send e-mail to target users. It searches for its e-mail recipients from files with the following extensions:

- HTM
- WAB
- HTM
- DBX
- TBB

It spoofs the e-mail address of the sender. It also includes an attachment (DOCUMENT.ZIP). As of this writing, its propagation routine does not appear to be functioning properly. It steals critical system and user information and sends all gathered data to a remote user. It runs on Windows 95, 98, ME, and XP.

**WORM\_MYDOOM.F (Aliases: MyDoon.F, W32/Mydoom.f@MM) (Win32 Worm):** This memory resident worm is almost similar to WORM\_MYDOOM.A. The only functional difference is that the Denial of Service (DoS) attack routine of this malware is designed to end on February 14, 2006 instead of February 12, 2004. It selects from a list of e-mail subjects, message bodies, and attachment file names for its e-mail messages. The worm spoofs the sender name of its messages so that they appear to have been sent by different users instead of the actual users on infected machines. It performs a Denial of Service (DoS) attack on the Web sites, www.microsoft.com and rias.com. This is triggered if the system date is February 1, 2004 or later and the system time is 4:09:18 PM (16:09:18). It continues its DoS attack until February 14, 2006 2:28:57 AM (02:28:57). On the said date, this worm will not perform most of its routines, except for its backdoor functionalities. This worm also attempts to install backdoor components by opening a listening port 1080. It may be waiting for remote malicious user to take control of the compromised machine. It is also able to open several ports ranging from 3000 to 5000, to connect to remote SMTP servers to send e-mail. It runs on Windows 95, 98, ME, NT, 2000, and XP.

**WORM\_NODOOM.A (Aliases: W32/Nodoom.a@MM, I-Worm.Nodoom, W32/TiniPOC.A.worm, Win32.Nodoom.A) (Internet Worm):** This memory-resident worm uses its own SMTP (Simple Mail Transfer Protocol) engine to send out e-mail messages. The e-mail message it sends out has various subject lines, message bodies, and attachments. It acquires its target e-mail addresses by searching for files that contain various extensions in an infected system. It runs on Windows 95, 98, ME, NT, 2000, and XP.

**WORM\_REDWA.A (Internet Worm):** This worm is a Windows executable version of BAT\_REDWA.A, a mass-mailing batch file malware. It spreads via e-mail, Internet Relay Chat (IRC), and peer-to-peer file-sharing applications. However, it fails to execute some of its intended routines due to programming errors. It sends copies of itself with the following details to all e-mail addresses found in the address book of a target user:

- Subject: Symantec Security Alert
- Attachment: Symantec\_W32\_Cure.bat

It also deletes several AntiVirus programs. It runs on Windows 95, 98, ME, NT, 2000, and XP.

**X97M.Ellar.F (Excel 97 Macro Virus):** This is a macro virus that infects Microsoft® Excel 97 and the template file. This virus also deletes some files and folders.

**X97M.Esab (Excel 97 Macro Virus):** This is a simple macro virus that creates the 0Killbase.xls file in the Microsoft® Excel startup folder. It infects other Excel workbooks when they are saved.

## 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.*

The Virus and Trojan sections are derived from compiling information from the following anti-virus vendors and security related web sites: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs and The WildList Organization International.

Trojan	Version	CyberNotes Issue #
Backdoor.Aphexdoor	N/A	CyberNotes-2004-03
<b>Backdoor.Domwis</b>	<b>N/A</b>	<b>Current Issue</b>
Backdoor.Gaster	N/A	CyberNotes-2004-01
Backdoor.Graybird.H	H	CyberNotes-2004-01
Backdoor.IRC.Aladinz.F	F	CyberNotes-2004-01
Backdoor.IRC.Aladinz.G	G	CyberNotes-2004-02
Backdoor.IRC.Aladinz.H	H	CyberNotes-2004-02
<b>Backdoor.IRC.Aladinz.J</b>	<b>J</b>	<b>Current Issue</b>
<b>Backdoor.OptixPro.13.C</b>	<b>13.C</b>	<b>Current Issue</b>
Backdoor.OptixPro.13b	13b	CyberNotes-2004-02
Backdoor.Portless	N/A	CyberNotes-2004-01
Backdoor.Sdbot.S	S	CyberNotes-2004-01
Backdoor.Threadsys	N/A	CyberNotes-2004-02
Backdoor.Trodal	N/A	CyberNotes-2004-01
Backdoor.Tuxder	N/A	CyberNotes-2004-02
BackDoor-AWQ.b	B	CyberNotes-2004-01
BackDoor-CBH	N/A	CyberNotes-2004-01
BDS/Purisca	N/A	CyberNotes-2004-01
BKDR_UPROOTKIT.A	A	CyberNotes-2004-01
Dial/ExDial-A	A	CyberNotes-2004-01
DOS_MASSMSG.A	A	CyberNotes-2004-01
Download.Berbew.dam	N/A	CyberNotes-2004-01
Downloader.Mimail.B	B	CyberNotes-2004-02
Downloader-GD	GD	CyberNotes-2004-01
Downloader-GH	GH	CyberNotes-2004-02
Downloader-GN	GN	CyberNotes-2004-02
Dyfuca	N/A	CyberNotes-2004-01
Exploit-URLSpooF	N/A	CyberNotes-2004-01
Hacktool.Sagic	N/A	CyberNotes-2004-01
IRC-Bun	N/A	CyberNotes-2004-01
JS/AdClicker-AB	AB	CyberNotes-2004-01
Keylogger.Stawin	N/A	CyberNotes-2004-03
<b>MultiDropper-GP.dr</b>	<b>GP.dr</b>	<b>Current Issue</b>
Needy.C	C	CyberNotes-2004-03
Ouch	N/A	CyberNotes-2004-02
Perl/Exploit-Sqlinject	N/A	CyberNotes-2004-01
<b>Phish-Potpor</b>	<b>N/A</b>	<b>Current Issue</b>
Proxy-Agent	N/A	CyberNotes-2004-03

Trojan	Version	CyberNotes Issue #
Proxy-Cidra	N/A	CyberNotes-2004-01
PWS-Datei	N/A	CyberNotes-2004-01
PWSteal.Bancos.D	D	CyberNotes-2004-01
PWSteal.Freemega	N/A	CyberNotes-2004-02
PWSteal.Leox	N/A	CyberNotes-2004-02
PWSteal.Olbaid	N/A	CyberNotes-2004-03
PWSteal.Sagic	N/A	CyberNotes-2004-01
<b>QReg-9</b>	<b>9</b>	<b>Current Issue</b>
Startpage-AI	AI	CyberNotes-2004-01
StartPage-AU	AU	CyberNotes-2004-02
StartPage-AX	AX	CyberNotes-2004-02
TR/DL906e	N/A	CyberNotes-2004-01
TR/Psyme.B	B	CyberNotes-2004-01
Troj/AdClick-Y	Y	CyberNotes-2004-03
Troj/Agent-C	C	CyberNotes-2004-01
Troj/Antikl-Dam	N/A	CyberNotes-2004-01
Troj/Apher-L	L	CyberNotes-2004-02
Troj/BeastDo-M	M	CyberNotes-2004-01
Troj/BeastDo-N	N	CyberNotes-2004-01
Troj/ByteVeri-E	E	CyberNotes-2004-03
Troj/Chapter-A	A	CyberNotes-2004-03
Troj/Cidra-A	A	CyberNotes-2004-01
Troj/Control-E	E	CyberNotes-2004-03
Troj/CoreFloo-D	D	CyberNotes-2004-01
Troj/Daemoni-B	B	CyberNotes-2004-03
Troj/Daemoni-C	C	CyberNotes-2004-03
Troj/Darium-A	A	CyberNotes-2004-01
<b>Troj/DDosSmal-B</b>	<b>B</b>	<b>Current Issue</b>
Troj/Delf-JV	JV	CyberNotes-2004-02
Troj/Delf-NJ	NJ	CyberNotes-2004-01
Troj/DelShare-G	G	CyberNotes-2004-01
Troj/Digits-B	B	CyberNotes-2004-03
Troj/Divix-A	A	CyberNotes-2004-02
Troj/Dloader-K	K	CyberNotes-2004-01
Troj/Femad-B	B	CyberNotes-2004-03
Troj/Femad-D	D	CyberNotes-2004-01
Troj/Flator-A	A	CyberNotes-2004-01
Troj/Flood-CR	CR	CyberNotes-2004-02
Troj/Flood-DZ	DZ	CyberNotes-2004-03
Troj/Getdial-A	A	CyberNotes-2004-01
Troj/Hackarmy-A	A	CyberNotes-2004-02
Troj/Hidemirc-A	A	CyberNotes-2004-03
Troj/Hosts-A	A	CyberNotes-2004-01
Troj/Hosts-B	B	CyberNotes-2004-02
Troj/IEStart-G	G	CyberNotes-2004-02
Troj/Inor-B	B	CyberNotes-2004-02
Troj/Ipons-A	A	CyberNotes-2004-01
Troj/Ircbot-S	S	CyberNotes-2004-02
Troj/IRCBot-U	U	CyberNotes-2004-03
Troj/Ircfloo-A	A	CyberNotes-2004-03
Troj/Ketch-A	A	CyberNotes-2004-01
Troj/Kuzey-A	A	CyberNotes-2004-02

Trojan	Version	CyberNotes Issue #
Troj/Lalus-A	A	CyberNotes-2004-01
Troj/Ldpinch-C	C	CyberNotes-2004-02
Troj/Legmir-E	E	CyberNotes-2004-01
Troj/Lindoor-A	A	CyberNotes-2004-02
Troj/Linplait-A	A	CyberNotes-2004-02
Troj/Mahru-A	A	CyberNotes-2004-03
Troj/Mircsend-A	A	CyberNotes-2004-02
Troj/Mmdload-A	A	CyberNotes-2004-02
Troj/MsnCrash-B	B	CyberNotes-2004-01
Troj/Mssvc-A	A	CyberNotes-2004-01
<b>Troj/Myss-C</b>	<b>C</b>	<b>Current Issue</b>
Troj/NoCheat-B	B	CyberNotes-2004-03
Troj/Noshare-K	K	CyberNotes-2004-02
<b>Troj/Pinbol-A</b>	<b>A</b>	<b>Current Issue</b>
Troj/Proxin-A	A	CyberNotes-2004-02
Troj/Saye-A	A	CyberNotes-2004-02
Troj/Sdbot-AP	AP	CyberNotes-2004-03
Troj/SdBot-BB	BB	CyberNotes-2004-02
Troj/Sdbot-CY	CY	CyberNotes-2004-01
Troj/Sdbot-EF	EF	CyberNotes-2004-01
Troj/SdBot-EG	EG	CyberNotes-2004-01
Troj/SdBot-EI	EI	CyberNotes-2004-01
Troj/Sdbot-EJ	EJ	CyberNotes-2004-02
Troj/Sdbot-EK	EK	CyberNotes-2004-02
Troj/Sdbot-EL	EL	CyberNotes-2004-02
<b>Troj/Sdbot-FM</b>	<b>FM</b>	<b>Current Issue</b>
Troj/Search-A	A	CyberNotes-2004-02
Troj/Sect-A	A	CyberNotes-2004-02
Troj/Seeker-F	F	CyberNotes-2004-01
Troj/Small-AW	AW	CyberNotes-2004-03
Troj/Spooner-C	C	CyberNotes-2004-02
Troj/SpyBot-AA	AA	CyberNotes-2004-01
Troj/Spybot-AM	AM	CyberNotes-2004-01
Troj/Spybot-C	C	CyberNotes-2004-01
Troj/StartPag-C	C	CyberNotes-2004-01
Troj/StartPag-E	E	CyberNotes-2004-02
Troj/StartPg-U	U	CyberNotes-2004-01
Troj/StartPg-AU	AU	CyberNotes-2004-01
Troj/StartPg-AY	AY	CyberNotes-2004-01
Troj/StartPg-BG	BG	CyberNotes-2004-01
Troj/Stawin-A	A	CyberNotes-2004-03
Troj/TCXMedi-E	E	CyberNotes-2004-01
Troj/Tofger-F	F	CyberNotes-2004-01
Troj/Tofger-L	L	CyberNotes-2004-01
Troj/Troll-A	A	CyberNotes-2004-02
Troj/Uproot-A	A	CyberNotes-2004-01
Troj/Volver-A	A	CyberNotes-2004-03
Troj/Weasyw-A	A	CyberNotes-2004-02
Troj/Webber-D	D	CyberNotes-2004-01
Troj/Winpup-C	C	CyberNotes-2004-03
Trojan.Anymail	N/A	CyberNotes-2004-01
<b>Trojan.Bansap</b>	<b>N/A</b>	<b>Current Issue</b>

Trojan	Version	CyberNotes Issue #
Trojan.Bookmarker	N/A	CyberNotes-2004-01
Trojan.Bookmarker.B	B	CyberNotes-2004-02
Trojan.Bookmarker.C	C	CyberNotes-2004-02
Trojan.Bookmarker.D	C	CyberNotes-2004-03
Trojan.Bookmarker.E	E	CyberNotes-2004-03
Trojan.Download.Revir	N/A	CyberNotes-2004-01
Trojan.Gema	N/A	CyberNotes-2004-01
<b>Trojan.Gutta</b>	<b>N/A</b>	<b>Current Issue</b>
Trojan.Httpdos	N/A	CyberNotes-2004-02
Trojan.Mitglieder.C	C	CyberNotes-2004-02
Trojan.PWS.Qphook	N/A	CyberNotes-2004-01
<b>Trojan.PWS.QQPass.F</b>	<b>F</b>	<b>Current Issue</b>
Unix/Exploit-SSHIDEN	N/A	CyberNotes-2004-02
UrlSpoof.E	E	CyberNotes-2004-03
<b>VBS.Bootconf.B</b>	<b>B</b>	<b>Current Issue</b>
VBS.Shania	N/A	CyberNotes-2004-03
VBS/Inor-C	C	CyberNotes-2004-03
VBS/Suzer-B	B	CyberNotes-2004-01
VBS/Wisis-A	A	CyberNotes-2004-02
W32.Bizten	N/A	CyberNotes-2004-01
W32.Hostidel.Trojan.B	B	CyberNotes-2004-03
<b>W32.Kifer</b>	<b>N/A</b>	<b>Current Issue</b>
<b>W32.Kifer.B</b>	<b>B</b>	<b>Current Issue</b>
Xombe	N/A	CyberNotes-2004-01

**Backdoor.Domwis:** This is a backdoor Trojan horse that allows unauthorized, remote access to your computer. By default it opens TCP port 559.

**Backdoor.IRC.Aladinz.J:** This is a backdoor Trojan horse that uses malicious scripts in the mIRC client software, allowing unauthorized remote access.

**Backdoor.OptixPro.13.C:** This Trojan horse gives a remote malicious user full access to your computer. By default, the Trojan opens TCP port 4001 for listening. When Backdoor.Domwis is executed, it opens TCP port 559, which allows unauthorized remote access to an infected computer. The Trojan copies itself as %Windir%\RUNDLL16.EXE and attempts to add the value, "Windows DLL Loader" = "%Windir%\RUNDLL16.EXE," to the registry key:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

so that the Trojan runs when you start Windows.

**MultiDropper-GP.dr (Alias: PHP\_BIZAI.A):** This Trojan simply installs other Trojans. It was being installed via an Internet Explorer exploit. Unsuspecting users who navigated to a specified website using a vulnerable web browser would become infected. At the time of this writing, the website in question is no longer responding. Upon visiting the infectious web page, the Exploit-MhtRedir Trojan would download and access a Microsoft Compiled Help file (CHM.CHM). Within this CHM file exists an HTML document LAUNCH.HTML, which contains the Exploit-CodeBase Trojan to run the file MSTASK.EXE, which is the MultiDropper-GP.a Trojan.

**Phish-Potpor:** This is a Trojan that sends out a huge amount of e-mails asking the recipient to update his Visa Card contact information including card number, name, expiration date, and PIN. When executed, the Trojan copies itself to %windir% folder using the filename "LPCONFIG.EXE." It creates a registry key so it gets started on system boot:

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
"ipconfig" = c:\winnt\ipconfig.exe

The e-mails have these properties:

- From: "VISA" [support@visa.com]
- Subject: "VISA Announcement!"

The Trojan contains a list of SMTP servers that it uses to submit the mails. When the 'here' link within the mail body is clicked, the browser will open a page hosted on a DYNDNS.ORG IP address.

**QReg-9 (Aliases: BruteCode, Win32.Lovmus, Win32/BruteCode):** This Trojan is written in MSVB, and is intended to alter various settings on the victim machine. It may be received with a .JPG.EXE file extension, intended to fool the user into thinking it is an image, not an executable file. When run, the Trojan copies itself as BCFOLDER.EXE to the system directory of the victim machine, for example:

- C:\WINNT\SYSTEM32\BCFOLDER.EXE

The following Registry key is modified to hook the Trojan:

- HKEY\_CLASSES\_ROOT\Folder\shell\open\command "(Default)"

It is changed from "%SystemRoot%\Explorer.exe /idlist,%I,%L" to "C:\WINNT\System32\BCfolder.exe explorer.exe /idlist,%I,%L." Additionally, the following Registry is modified, renaming the Recycle Bin on the victim machine:

- HKEY\_CLASSES\_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}  
"(Default)"

It is changed from "Recycle Bin" to [brutecode@yahoo.com](mailto:brutecode@yahoo.com). Similarly, the following key is also modified:

- HKEY\_CLASSES\_ROOT\CLSID\{645FF040-5081-101B-9F08-00AA002F954E}  
"LocalizedString"

From "@C:\WINNT\system32\shell32.dll,-8964@1033,Recycle Bin" to [brutecode@yahoo.com](mailto:brutecode@yahoo.com). The following important data is removed:

- HKEY\_CLASSES\_ROOT\Folder\shell\open\ddeexec "(Default)" = [ViewFolder("%I," %I, %S)]

Initial analysis suggests the Trojan is also intended to alter the default start page of Internet Explorer, although this was not observed in testing. The Trojan contains the string "Dedicated to: GOD'S\_OWN\_COUNTRY."

**Troj/DDosSmal-B:** This is a Trojan that attempts a Denial of Service attack on a website. In order to run automatically when Windows starts up the Trojan copies itself to the file winsys.exe in the Windows folder and adds the following registry entry:

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

**Troj/Myss-C (Aliases: TrojanDownloader.Win32.Donn.r, Downloader-DS):** This is a simple Trojan that overwrites the file Windows\Hosts.sam under Windows 95/98/ME, and Windows\System32\Drivers\etc\hosts under Windows NT/2000/XP based systems with '127.0.0.1 localhost.' It will then attempt to download and run the file Sys.exe from <http://teens3.com/dialler/new2/1/m121689.mpg>.

**Troj/Pinbol-A:** This is an IRC backdoor Trojan. When Troj/Pinbol-A is first executed, a copy is created in the Windows folder with the filename smvc32.exe and the following registry entry is created so that the Trojan is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\SMVC = smvc32.exe

Troj/Pinbol-A connects to a channel on a remote IRC server enabling a malicious user to gain unauthorized access to the victim's machine. It will store e-mail addresses harvested from the victim's computer in the file C:\cyclop.bin and periodically e-mail this information to the malicious user. A proxy server is set up on

a random port number that is stored in the registry at HKCU\Software\socks. The Trojan will also create the following registry entry:

- HKCU\Software\magic = 666.

**Troj/Sdbot-FM (Aliases: Backdoor.SdBot.gen, BKDR\_Sdbot.Gen):** This is a backdoor Trojan that runs in the background as a service process and allows unauthorized remote access to the computer via IRC channels. It copies itself to the Windows system folder as svch0st.exe and creates entries in the registry at the following locations to run itself on system restart:

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

The Trojan remains resident, listening for commands from remote users. If it receives the appropriate command the Trojan attempts to drop and execute a batch file detected as Bat/Botsecure-A in order to change the user's security settings.

**Trojan.Bansap:** This is a Trojan Horse that overwrites files with copies of itself.

**Trojan.Gutta:** This is a Trojan horse that disables access to .exe files. When this Trojan runs, it copies itself as C:\Windows\CSRSS.exe. This path is hard-coded and does not depend on system variables. The Trojan creates the value, "rundll32" = "windows\csrss.exe," in the registry key:

- HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

so that the Trojan attempts to start when you start Windows. It modifies the value of (Default) in the registry key:

- HKEY\_CLASSES\_ROOT\exefile\shell\open\command

by adding, hahafool, to the Value data. As a result, when you try to run a .exe file, it will not open. For example, if you try to run Notepad.exe after the modification is made, instead of looking for Notepad.exe, it looks for Notepad.exehahafool. This Trojan horse does not have backdoor or worm functionality. Because it modifies access to .exe files, it cannot run when Windows is restarted, but will generate an error message.

**Trojan.PWS.QQPass.F:** This is a password-stealing Trojan horse that steals passwords and user information. It is a Visual Basic (VB) application that requires the presence of the Microsoft VB run-time libraries for it to run.

**VBS.Bootconf.B:** This is a Trojan horse that modifies Internet Explorer settings, redirects Web sites such as Google, Yahoo and MSN to a different search page, and may pop up browser windows to a pornographic Web site.

**W32.Kifer (Alias: TrojanDropper.Win32.Kifer):** This is a Trojan horse that drops BAT.Snoital@mm, which will attempt to delete antiviral software from your computer. It also spreads through MAPI-enabled e-mail clients, such as Microsoft Outlook, and IRC. The e-mail has the following characteristics:

- Subject: Symantec Security Alert
- Attachment: Symantec\_W32\_Cure.bat

**W32.Kifer.B:** This is a Trojan Horse that uses Visual Basic (VB) scripts to attempt to mail itself to the addresses it finds in the Windows® Address Book. It also spreads through file-sharing programs, such as Kazaa®, BearShare®, and LimeWire®. The e-mail will have the following characteristics:

- Subject: Symantec Security Alert
- Attachment: Symantec\_Support.exe