

# US-CERT Cyber Security Bulletin

SB04-189

July 7, 2004

Information previously published in CyberNotes has been incorporated into US-CERT Cyber Security Bulletins, which are available from the US-CERT web site at <http://www.us-cert.gov/cas/bulletins/index.html>. You can also receive this information through e-mail by joining the Cyber Security Bulletin mailing list. Instructions are located at <http://www.us-cert.gov/cas/signup.html#tb>.

## Bugs, Holes & Patches

The following tables provide a summary of software vulnerabilities identified between June 21 and July 6, 2004. The tables provides the risk, vendor and software name, potential vulnerability/impact, any identified patches/workarounds/alerts and whether attacks have utilized this vulnerability or an exploit script is known to exist and the common name/CVE number. Software versions and operating systems are identified if known. The tables are organized by operating system with new information identified first followed by updated information. **Updates to items appearing in previous issues of CyberNotes/Cyber Security Bulletins 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. *Note: All the information included in the following tables has been discussed in newsgroups and websites.*

### Windows Operating Systems

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	CutePHP <sup>1</sup>  CuteNews 0.88, 1.3, 1.3.1	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of the 'id' parameter in certain scripts, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  <b>Proofs of Concept exploits have been published.</b>	CuteNews Multiple Cross-Site Scripting
<b>High</b>	IBM <sup>2</sup>  Lotus Notes 5.0.12, 6.0, 6.0.1, 6.5	A Cross-Site Scripting vulnerability exists because the Notes URL handler does not properly filter user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code.  Update available at: <a href="http://www-1.ibm.com/support/docview.wss?rs=463&amp;uid=swg21169510">http://www-1.ibm.com/support/docview.wss?rs=463&amp;uid=swg21169510</a>  <b>There is no exploit code required.</b>	IBM Lotus Notes URI Handler Cross-Site Scripting  <b>CVE Name: CAN-2004-0480</b>
<b>High</b>	Jelsoft Enterprises <sup>3</sup>  VBulletin 3.0.1	A Cross-Site Scripting vulnerability exists in the 'newreply.php' and 'newthread.php' scripts 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.  <b>There is no exploit code required; however, a Proof of Concept exploit has been published.</b>	VBulletin the 'newreply.php' & 'newthread.php' Cross-Site Scripting

<sup>1</sup> Securiteam, June 28, 2004.

<sup>2</sup> iDEFENSE Security Advisory, June 23, 2004.

<sup>3</sup> Securiteam, June 28, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	Jelsoft Enterprises <sup>4</sup>  vBulletin 3.0, Gamma, beta2-beta7, 3.0.1	A Cross-Site Scripting vulnerability exists in the 'newreply.php' script due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  There is no exploit code required.	vBulletin newreply.php Cross-Site Scripting
<b>High</b>	McMurtrey/Whitaker & Associates <sup>5</sup>  Cart32 2.5 a, 2.6, 3.0, 3.1, 3.5 a Build 710, 3.5 a, 3.5 Build 619, 3.5, 4.4, 5.0	A Cross-Site Scripting vulnerability exists in the 'cart32.exe' and 'c32web.exe' CGI scripts due to improper filtering of HTML code from 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.  There is no exploit code required; however, a Proof of Concept exploit has been published.	McMurtrey/Whitaker & Associates Cart32 Cross-Site Scripting
<b>High</b>	Microsoft <sup>6</sup>  Internet Explorer 5.0, 5.0.1, SP1-SP4, 5.5, SP1&SP2, 6.0, SP1	A zone bypass vulnerability exists when a remote malicious user uses a non-FQDN URI, which could lead to the execution of arbitrary code.  No workaround or patch available at time of publishing.  Proofs of Concept exploit scripts have been published.	Microsoft Internet Explorer Non-FQDN URI
<b>High</b>	Microsoft <sup>7</sup>  Internet Explorer 5.5 SP1&SP2, 6.0, SP1	A vulnerability exists that could permit malicious HTML documents to create or overwrite files on a victim file system when interpreted from the Local Zone (or other Security Zones with relaxed security restrictions, such as the Intranet Zone). This weakness depends on scripting that abuses the 'ADODB.Stream' Object. Exploitation of this weakness requires other vulnerabilities to redirect the browser into the Local Zone (or other appropriate Security Zone) and then reference the malicious content once it has been written to the client file system. A remote malicious user could execute arbitrary code.  For information on how to disable the ADODB.Stream object from Internet Explorer, see KB Article located at: <a href="http://support.microsoft.com/?kbid=870669">http://support.microsoft.com/?kbid=870669</a>  Numerous exploits in the wild take advantage of this and other security issues to install and execute malicious code on client systems. There are also a number of worms that have incorporated exploits for this and other security issues. Vulnerability has appeared in the press and other public media.	Microsoft Internet Explorer ADODB.Stream Object File Installation
<b>High</b>	Microsoft <sup>8</sup>  Internet Explorer 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists because it is possible to alter the registry to allow for previously patched vulnerabilities to be exploitable again, which could let a malicious user execute arbitrary script code.  No workaround or patch available at time of publishing.  Proofs of Concept exploits have been published.	Microsoft Internet Explorer Shell.Application Object Script Execution

<sup>4</sup> SecurityFocus, June 26, 2004.

<sup>5</sup> Securiteam, June 28, 2004.

<sup>6</sup> SecurityFocus, June 21, 2004.

<sup>7</sup> TA04-184A, <http://www.us-cert.gov/cas/techalerts/TA04-184A.html>

<sup>8</sup> Bugtraq, July 3, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	Netegrity <sup>9</sup>  IdentityMinder Web Edition 5.6, SP1&SP2, Policy Server 5.5	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  There is no exploit code required; however, Proofs of Concept exploits have been published.	IdentityMinder Cross-Site Scripting
<b>High</b>	SIMM-Comm <sup>10</sup>  SCI Photo Chat 3.4.9	A Cross-Site Scripting vulnerability exists in the web server component due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  There is no exploit code required; however, a Proof of Concept exploit has been published.	SCI Photo Chat Server Cross-Site Scripting
<b>High</b>	The Miller Group <sup>11</sup>  Centre 0.92, 1.0 1, 1.0	A vulnerability exists in 'modules.php' due to insufficient validation of the location of the user-supplied 'modname' parameter, which could let a remote malicious user execute arbitrary PHP code.  Upgrade available at: <a href="http://www.miller-group.net/">http://www.miller-group.net/</a>  A Proof of Concept exploit has been published.	Centre 'modules.php' Remote PHP Code Execution
<b>High/Medium</b>  (High if arbitrary code can be executed; and Medium is sensitive information can be obtained, comments deleted, Or journal entries added)	Francisco Burzi <sup>12</sup>  PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1 a, 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5, RC1-RC3, BETA1, FINAL, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1-7.3	Multiple vulnerabilities exist: a vulnerability exists because path information can be disclosed in error pages by passing invalid input or accessing scripts directly, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'modules/Journal/search.php' due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists because several Journal scripts do not filter HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists because the 'modules/Journal/commentkill.php' script does not require authentication, which could let a remote malicious user delete comments; and a vulnerability exists in 'modules/Journal/savenew.php' due to insufficient authentication, which could let a remote malicious user add new journal entries.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proofs of Concept exploits have been published.	PHP-Nuke Multiple Vulnerabilities

<sup>9</sup> SecurityTracker Alert, 1010633, July 2, 2004.

<sup>10</sup> Secunia Advisory, SA12015, July 6, 2004.

<sup>11</sup> SecurityTracker Alert, 1010634, July 3, 2004.

<sup>12</sup> Secunia Advisory, SA11920, June 23, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Medium</b></p> <p>(High if arbitrary code can be executed; and Medium is sensitive information can be obtained)</p>	<p>OSTicket.com<sup>13</sup></p> <p>osTicket STS 1.2</p>	<p>Multiple vulnerabilities exist: a vulnerability exists because attachments that are submitted as part of a support ticket request are stored with a predictable name in a known web location, which could let a remote malicious user obtain sensitive information; a vulnerability exists because users are not required to validate e-mail used to open a ticket via the on-line form, which could let a remote malicious user execute arbitrary code; and a vulnerability exist because file upload size limitations can be bypassed, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrade available at: <a href="http://www.osticket.com/downloads/osticket_1.2.7.zip">http://www.osticket.com/downloads/osticket_1.2.7.zip</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>OSTicket Multiple Vulnerabilities</p>
<p><b>High/Medium</b></p> <p>(Medium if arbitrary code can be executed; and Medium is sensitive information can be obtained)</p>	<p>PowerPortal<sup>14</sup></p> <p>PowerPortal 1.1 b, 1.3 b, 1.3</p>	<p>Multiple vulnerabilities exist: multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability exists in the 'modules.php' script, which could let a remote malicious user obtain sensitive information; and an information disclosure vulnerability exists because a remote malicious user can determine the installation path.</p> <p>No workaround or patch available at time of publishing</p> <p>Proofs of Concept exploits have been published.</p>	<p>PowerPortal Multiple Input Validation</p>
<p><b>High/Low</b></p> <p>(High if arbitrary code can be executed; and Low if a DoS)</p>	<p>ISC<sup>15</sup></p> <p>Fedora<sup>16</sup></p> <p>Mandrake<sup>17</sup></p> <p>SuSE<sup>18</sup></p> <p>ISC DHCPD 3.0.1 rc12 &amp; rc13;</p> <p>RedHat Fedora Core2;</p> <p>SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, x86_64, 9.1,</p> <p>Admin-CD for Firewall ,</p> <p>Connectivity Server, Database Server, Enterprise Server 8, 7, Firewall on CD, Office Server, SuSE eMail Server III</p>	<p>Several vulnerabilities exist: a buffer overflow vulnerability exists in routines that are responsible for logging hostname options, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a buffer overflow vulnerability exists on systems that lack a 'vsprintf()' library function (ISC DHCPD defines vsprintf as: #define vsprintf(buf, size, fmt, list) vsprintf (buf, fmt, list) , which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Upgrade available at: <a href="ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.1rc14.tar.gz">ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.1rc14.tar.gz</a></p> <p><b>Fedora:</b> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</a></p> <p><b>Mandrake:</b> <a href="http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:061">http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:061</a></p> <p><b>SuSE:</b> <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>ISC DHCP Remote Buffer Overflows</p> <p>CVE Names: CAN-2004-0460, CAN-2004-0461</p>

<sup>13</sup> osTicket Security Alert, June 26, 2004.

<sup>14</sup> Secunia Advisory, SA11960, June 29, 2004.

<sup>15</sup> Technical Cyber Security Alert TA04-174A, <http://www.us-cert.gov/cas/techalerts/TA04-174A.html>.

<sup>16</sup> Fedora Update Notification, FEDORA-2004-190, June 23, 2004.

<sup>17</sup> Mandrake Security Advisory, MDKSA-2004:06, June 22, 2004.

<sup>18</sup> SUSE Security Announcement, SuSE-SA:2004:019, June 22, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	BEA Systems, Inc. <sup>19</sup>  WebLogic Express 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Express for Win32 7.0, SP1-SP5, 8.1, SP1&SP2, Weblogic Server 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Server for Win32 7.0, SP1-SP5, 8.1, SP1&SP2	A vulnerability exists if a '<role-name>' within a '<security-constraint>' has specified a '*' as role name, which could let a remote malicious user obtain unauthorized access.  Patches available at: <a href="ftp://ftpna.beasys.com/pub/releases/security/CR175310_700sp5.jar">ftp://ftpna.beasys.com/pub/releases/security/CR175310_700sp5.jar</a> <a href="ftp://ftpna.beasys.com/pub/releases/security/CR175310_810sp2.jar">ftp://ftpna.beasys.com/pub/releases/security/CR175310_810sp2.jar</a>  There is no exploit code required.	BEA WebLogic Server & WebLogic Express role-name Unauthorized Access
Medium	CGIScript.NET <sup>20</sup>  csFAQ, 1.0	A vulnerability exists in 'csFAQ.cgi' due to insufficient handling of the 'database' parameter, which could let a remote malicious user obtain sensitive information.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proof of Concept exploit has been published.	csFAQ Installation Path Disclosure
Medium	IBM <sup>21</sup>  Lotus Domino 6.5.0, 6.5.1	A vulnerability exists in the 'setquota' command, which could let a remote malicious user alter their mail storage quota values.  No workaround or patch available at time of publishing.  There is no exploit code required.	IBM Lotus Domino IMAP Quota Changing
Medium	Microsoft <sup>22</sup>  Internet Explorer 5.0.1, SP1-SP4, 5.5, SP1&SP2, 6.0, SP1	A vulnerability exists due to a failure to stop a malicious website from loading arbitrary content in a frame in another browser window, which could let a remote malicious user load arbitrary content that appears to originate from a trusted site.  No workaround or patch available at time of publishing  A Proof of Concept exploit has been published.	Microsoft Internet Explorer Cross-Domain Frame Loading
Medium	Phpmyfamily <sup>23</sup>  phpmyfamily 1.2.4, 1.2.5, 1.3	A vulnerability exists when the 'registers_globals' PHP configuration directive is enabled, which could let a remote malicious user obtain elevated privileges.  Upgrades available at: <a href="http://www.phpmyfamily.net/downloads.php">http://www.phpmyfamily.net/downloads.php</a>  There is no exploit code required.	PHPMyFamily Authentication Bypass

<sup>19</sup> BEA Systems Security Advisory, BEA04-64.00, June 28, 2004.

<sup>20</sup> Bugtraq, June 28, 2004.

<sup>21</sup> Bugtraq, June 30, 2004.

<sup>22</sup> Bugtraq, June 29, 2004.

<sup>23</sup> Secunia Advisory, SA11944, June 28, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	Qbik IP Management Limited <sup>24</sup>  WinGate Plus 5.0.5, 5.2.3 Build 901, 6.0 Beta 2 Build 942, 5.0.5, 5.2.3 Build 901, 6.0 Beta 2 Build 942	A Directory Traversal vulnerability exists in the HTTP proxy server, which could let a remote malicious user obtain sensitive information.  Upgrades available at: <a href="http://www334.pair.com/qbiknz/downloads/WinGate6.0.0.963-USE.EXE">http://www334.pair.com/qbiknz/downloads/WinGate6.0.0.963-USE.EXE</a>  There is no exploit code required.	WinGate Directory Traversal  CVE Names: CAN-2004-0577, CAN-2004-0578
Medium	ZaireWeb Solutions <sup>25</sup>  Newsletter ZWS	A vulnerability exists in the 'admin.php' script due to a design error in the implementation of the authentication system, which could let a remote malicious user bypass the administrative interface authentication.  No workaround or patch available at time of publishing.  A Proof of Concept exploit has been published.	ZaireWeb Solutions Newsletter ZWS Administrative Interface Authentication Bypass
Medium/ Low  (Medium if unauth- orized access can be obtained; and Low if a DoS)	NewAtlanta <sup>26</sup>  ServletExec 2.2, 3.0	A vulnerability exists due to an access validation error, which could let a malicious user obtain unauthorized access and possibly cause a Denial of Service.  No workaround or patch available at time of publishing  Currently we are not aware of any exploits for this vulnerability.	New Atlanta ServletExec Unauthorized Access
Low	Apache Software Foundation Apple Mandrake <sup>27</sup> Trustix <sup>28</sup>  Apache 2.0.47-2.0.49	A remote Denial of Service vulnerability exists in the 'ap_get_mime_headers_core()' function due to a failure to handle excessively long HTTP header strings.  Patches available at: <a href="http://www.apache.org/dist/httpd/patches/apply_to_2.0.49/CAN-2004-0493.patch">http://www.apache.org/dist/httpd/patches/apply_to_2.0.49/CAN-2004-0493.patch</a> <b>Mandrake:</b> <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a> <b>Trustix:</b> <a href="ftp://ftp.rustix.org/pub/trustix/updates/">ftp://ftp.rustix.org/pub/trustix/updates/</a>  Currently we are not aware of any exploits for this vulnerability.	Apache ap_escape_html Remote Denial of Service  CVE Name: CAN-2004-0493

<sup>24</sup> iDEFENSE Security Advisory , July 1, 2004.

<sup>25</sup> Bugtraq, June 24, 2004.

<sup>26</sup> SecurityFocus, June 30, 2004.

<sup>27</sup> Mandrakelinux Security Update Advisory , MDKSA-2004:064, June 29, 2004.

<sup>28</sup> Trustix Security Advisory, TSL-2004-0038, June 29, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	EFS Software, Inc. <sup>29</sup>  Easy Chat Server 1.0, 1.1, 1.2	Multiple Denial of Service vulnerabilities exist due to insufficient sanitization of user-supplied URI data and the inability to handle large numbers of anonymous users created in chat rooms.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proof of Concept exploit has been published.	Easy Chat Server Denial of Service
Low	IBM <sup>30</sup>  Lotus Domino 6.5.1	A remote Denial of Service vulnerability exists when a malicious user's e-mail is opened through the Domino Web Access.  No workaround or patch available at time of publishing.  A Proof of Concept exploit has been published.	IBM Lotus Domino Malicious Email Remote Denial of Service
Low	IBM <sup>31</sup>  WebSphere Caching Proxy Server 5.0 2, Edge server Caching proxy 5.0 2	A Denial of Service vulnerability exists in the Caching Proxy component due to a failure to handle incomplete 'GET' requests, if the 'JunctionRewrite' and 'UseCookie' directives are active.  IBM reportedly plans to release a fixed version (5.0.3). Also, IBM customers with Support Level 2 or 3 can request a patch.  There is no exploit code required; however, a Proof of Concept exploit has been published.	IBM WebSphere Edge Server Component Caching Proxy Denial of Service
Low	Sun Microsystems, Inc. <sup>32</sup>  Sun JRE (Linux Production Release) 1.4.1_01-1.4.1_03, 1.4.1, 1.4.2_01-1.4.2_04, 1.4.2, JRE (Solaris Production Release) 1.4.1_01-1.4.1_03, 1.4.1, 1.4.2_01-1.4.2_04, 1.4.2, JRE (Windows Production Release) 1.4.1_01-1.4.1_03, 1.4.1_07, 1.4.1, 1.4.2_01-1.4.2_04, 1.4.2	A Denial of Service vulnerability exists in the Sun Java Runtime Environment Font object due to a failure to handle exceptional conditions when processing font objects.  No workaround or patch available at time of publishing.  A Proof of Concept exploit script has been published.	Sun Java Runtime Environment Font Object Denial of Service

<sup>29</sup> Securiteam, July 4, 2004.

<sup>30</sup> Bugtraq, June 30, 2004.

<sup>31</sup> CYBSEC Security Advisory, July 2, 2004.

<sup>32</sup> SecurityFocus, June 28, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/ Medium</b></p> <p><b>(Medium if sensitive information can be obtained or corrupted)</b></p>	<p>Invision Power Services<sup>33</sup></p> <p>Invision Board 1.3.1 Final</p> <p><i>Upgrade now available<sup>34</sup></i></p>	<p>An input validation vulnerability exists in 'ssi.php' due to insufficient validation or user-supplied input, which could let a remote malicious user obtain/modify sensitive information or execute arbitrary commands.</p> <p><i>Upgrade available at:</i> <a href="http://forums.invisionpower.com/index.php?act=Attach&amp;type=post&amp;id=1096">http://forums.invisionpower.com/index.php?act=Attach&amp;type=post&amp;id=1096</a></p> <p><b>There is no exploit code required; however, a Proof of Concept exploit has been published.</b></p>	<p>Invision Power Board Input Validation</p>
<p><b>High/Low</b></p> <p><b>(High if arbitrary code can be executed)</b></p>	<p>Apache Software Foundation<sup>35</sup></p> <p><i>Gentoo<sup>36</sup></i> <i>Mandrake<sup>37</sup></i> <i>OpenBSD</i> <i>OpenPKG<sup>38</sup></i> <i>RedHat<sup>39</sup></i> <i>SGI<sup>40</sup></i> <i>Tinysofa<sup>41</sup></i> <i>Trustix<sup>42</sup></i></p> <p>Apache 1.3-2.0.49</p> <p><i>More vendor advisories issued</i></p>	<p>A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.</p> <p>No workaround or patch available at time of publishing.</p> <p><b>Currently we are not aware of any exploits for this vulnerability.</b></p> <p><i>Patch available at:</i> <a href="http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&amp;r2=1.106">http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&amp;r2=1.106</a></p> <p><i>Mandrake:</i> <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a></p> <p><i>OpenPKG:</i> <a href="ftp://ftp.openpkg.org">ftp://ftp.openpkg.org</a></p> <p><i>Tinysofa:</i> <a href="http://www.tinysofa.org/support/errata/2004/008.html">http://www.tinysofa.org/support/errata/2004/008.html</a></p> <p><i>Trustix:</i> <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p><i>Gentoo:</i> <a href="http://security.gentoo.org/glsa/glsa-200406-05.xml">http://security.gentoo.org/glsa/glsa-200406-05.xml</a></p> <p><i>OpenBSD:</i> <a href="http://www.openbsd.org/errata.html">http://www.openbsd.org/errata.html</a></p> <p><i>SGI:</i> <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/">ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/</a></p>	<p>Apache Mod_SSL SSL_Util_UUEn code_Binary Stack Buffer Overflow Vulnerability</p> <p><b>CVE Name: CAN-2004-0488</b></p>

<sup>33</sup> SecurityTracker Alert, 1010448, June 9, 2004.

<sup>34</sup> SecurityFocus, June 30, 2004.

<sup>35</sup> Security Focus, May 17, 2004

<sup>36</sup> Gentoo Linux Security Advisory , GLSA 200406-05, June 9, 2004.

<sup>37</sup> Mandrakelinux Security Update Advisories, MDKSA-2004:054 & 055, June 1, 2004.

<sup>38</sup> OpenPKG Security Advisory, OpenPKG-SA-2004.026, May 27, 2004.

<sup>39</sup> RedHat Security Advisory, RHSA-2004:342-10, July 6, 2004.

<sup>40</sup> SGI Security Advisory , 20040605-01-U, June 21, 2004.

<sup>41</sup> Tinysofa Security Advisory, TSSA-2004-008, June 2, 2004.

<sup>42</sup> Trustix Security Advisory, TSLSA-2004-0031, June 2, 2004.

Risk*	Vendor & Software Name	Windows Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(Low if a DoS)</b></p>	<p>Epic Games<sup>43</sup></p> <p>ARUSH Devastation 390.0; DreamForge TNN; Outdoors Pro Hunter; Epic Games Unreal Engine 436, 433, 226f, Unreal Tournament 451b, 2003 2225 win32, 2225 macOS, 2199 win32, 2199 macOS, 2199 linux, 2004 win32, macOS; nfogrames TacticalOps 3.4 Infogrames X-com Enforcer; Ion Storm DeusEx 1.112 fm; Nerf Arena Blast Nerf Arena Blast 1.2; Rage Software Mobile Forces 20000.0; Robert Jordan Wheel of Time 333.0 b; Running With Scissors Postal 2 1337</p> <p><i>Exploit script published<sup>44</sup></i></p>	<p>A buffer overflow vulnerability exists when a specially crafted ‘Secure’ query is submitted via a UDP with a long ‘query’ value, which could let a remote malicious user cause a Denial of Service and execute arbitrary code.</p> <p>Patches available at:: Unreal Tournament 2004 win32 <a href="http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120">http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120</a> Epic Games Unreal Tournament 2004 macOS: <a href="http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120">http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120</a></p> <p><i>Exploit script has been published.</i></p>	<p>Epic Games Unreal Engine ‘Secure’ Query Buffer Overflow</p>

<sup>43</sup> SecurityTracker Alert, 1010535, June 18, 2004.

<sup>44</sup> SecurityFocus, June 23, 2004.

## Unix Operating Systems

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	CutePHP <sup>45</sup>  CuteNews 0.88, 1.3, 1.3.1	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of the 'id' parameter in certain scripts, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  <i>Proofs of Concept exploits have been published.</i>	CuteNews Multiple Cross-Site Scripting
<b>High</b>	Dave White <sup>46</sup>  Dr. Cat 0.5 .0-beta	Multiple buffer overflow vulnerabilities exist in the 'drcatd' daemon due to insufficient boundary checks, which could let a malicious user execute arbitrary code.  No workaround or patch available at time of publishing.  <i>Currently we are not aware of any exploits for this vulnerability.</i>	Dr.Cat Drcatd Multiple Local Buffer Overflows
<b>High</b>	Double Precision, Inc. <sup>47</sup>  SqWebMail 4.0.4 .20040524	A Cross-Site Scripting vulnerability exists in the 'print_header_uc()' function in 'folder.c' due to insufficient sanitization of user-supplied e-mail header strings, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  <i>A Proof of Concept exploit has been published.</i>	SqWebMail Email Header Cross-Site Scripting  <b>CVE Name:</b> <b>CAN-2004-0591</b>
<b>High</b>	GNU Gentoo <sup>48</sup>  gzip 1.3.3	A vulnerability exists in the 'gzexe' script due to insecure creation of temporary files, which could let a local/remote malicious user execute arbitrary commands.  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200406-18.xml">http://security.gentoo.org/glsa/glsa-200406-18.xml</a>  <i>There is no exploit code required.</i>	GNU 'gzexe' Insecure Temporary File Creation  <b>CVE Name:</b> <b>CAN-2004-0603</b>
<b>High</b>	GNU <sup>49</sup>  GNATS 3.0 02, 3.2, 3.14 b, 3.113 .1_6, 3.113, 3.113.1, 4.0	A format string vulnerability exists in 'misc.c,' which could let a malicious user execute arbitrary code.  No workaround or patch available at time of publishing.  <i>Currently we are not aware of any exploits for this vulnerability.</i>	GNU GNATS Format String
<b>High</b>	IBM <sup>50</sup>  Informix I-Spy 2.0	A vulnerability exists in the 'runbin' binary, which could let a malicious user obtain ROOT access.  Fix available at: <a href="http://www-1.ibm.com/support/docview.wss?uid=swg21172742&amp;aid=1">http://www-1.ibm.com/support/docview.wss?uid=swg21172742&amp;aid=1</a>  <i>There is no exploit code required.</i>	IBM Informix I-Spy 'runbin' Root Privileges

<sup>45</sup> Securiteam, June 28, 2004.

<sup>46</sup> Securiteam, June 28, 2004.

<sup>47</sup> SecurityTracker Alert, 1010560, June 24, 2004.

<sup>48</sup> Gentoo Linux Security Advisory , GLSA 200406-18, June 24, 2004.

<sup>49</sup> Zone-h Security Advisory , ZH2004-11SA, June 25, 2004.

<sup>50</sup> SecurityFocus, July 2, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	James Henstridge Debian <sup>51</sup>  www-sql 0.5.7	A buffer overflow vulnerability exists in 'cgi.c,' due to a failure to properly handle user-supplied strings when copying them into finite stack-based buffers, which could let a malicious user execute arbitrary code.  <b>Debian:</b> <a href="http://security.debian.org/pool/updates/main/w/www-sql/">http://security.debian.org/pool/updates/main/w/www-sql/</a>  Currently we are not aware of any exploits for this vulnerability.	WWW-SQL Include Command Buffer Overflow  CVE Name: CAN-2004-0455
<b>High</b>	Jelsoft Enterprises <sup>52</sup>  VBulletin 3.0.1	A Cross-Site Scripting vulnerability exists in the 'newreply.php' and 'newthread.php' scripts 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.  There is no exploit code required; however, a Proof of Concept exploit has been published.	VBulletin the 'newreply.php' & 'newthread.php' Cross-Site Scripting
<b>High</b>	Jelsoft Enterprises <sup>53</sup>  VBulletin 3.0, Gamma, beta2-beta7, 3.0.1	A Cross-Site Scripting vulnerability exists in the 'newreply.php' script due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  There is no exploit code required.	vBulletin newreply.php Cross-Site Scripting
<b>High</b>	Netegrity <sup>54</sup>  IdentityMinder Web Edition 5.6, SP1&SP2, Policy Server 5.5	Multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  No workaround or patch available at time of publishing.  There is no exploit code required; however, Proofs of Concept exploits have been published.	IdentityMinder Cross-Site Scripting
<b>High</b>	Open Webmail <sup>55</sup>  Open Webmail 1.7, 1.8, 1.71, 1.81, 1.90, 2.20, 2.21, 2.30-2.32	A vulnerability exists in the 'vacation.pl' component due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary code.  Patch available at: <a href="http://openwebmail.org/openwebmail/download/cert/patches/SA-04:04/vacation.pl.patch">http://openwebmail.org/openwebmail/download/cert/patches/SA-04:04/vacation.pl.patch</a>  There is no exploit code required.	Open WebMail 'Vacation.pl' Input Validation

<sup>51</sup> Debian Security Advisory, DSA 523-1, June 19, 2004.

<sup>52</sup> Securiteam, June 28, 2004.

<sup>53</sup> SecurityFocus, June 26, 2004.

<sup>54</sup> SecurityTracker Alert, 1010633, July 2, 2004.

<sup>55</sup> Open Webmail Security Advisory, 20040629, June 28, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	pavuk.sourceforge.net Debian <sup>56</sup> Gentoo <sup>57</sup>  Pavuk 0.9pl28i, 0.928r1; Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, ia-32, hppa, arm, alpha; Gentoo Linux 1.1 a, 1.2, 1.4, rc1-rc3	A buffer overflow vulnerability exists due to a boundary error when processing HTTP 'Location:' header information, which could let a remote malicious user execute arbitrary code.  <b>Debian:</b> <a href="http://security.debian.org/pool/updates/main/p/pavuk/">http://security.debian.org/pool/updates/main/p/pavuk/</a> <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200406-22.xml">http://security.gentoo.org/glsa/glsa-200406-22.xml</a>  Currently we are not aware of any exploits for this vulnerability.	Pavuk Remote 'Location:' Header Remote Buffer Overflow  <b>CVE Name:</b> <b>CAN-2004-0456</b>
<b>High</b>	phpMyAdmin <sup>58</sup>  phpMyAdmin 2.5.1, 2.5.2, 2.5.4, 2.5.5 pl1, 2.5.5 -rc1&rc2, 2.5.5, 2.5.6 -rc1, 2.5.7	Multiple input validation vulnerabilities exist: a vulnerability exists in the 'left.php' script due to insufficient sanitization of user-supplied input, which could let a remote malicious user add arbitrary servers; and a vulnerability exists in the PHP 'eval()' statement, which could let a remote malicious user execute arbitrary PHP code.  Upgrades available at: <a href="http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.5.7-pl1.tar.gz?download">http://prdownloads.sourceforge.net/phpmyadmin/phpMyAdmin-2.5.7-pl1.tar.gz?download</a>  Exploit script has been published.	phpMyAdmin Multiple Input Validation
<b>High</b>	SIMM-Comm <sup>59</sup>  SCI Photo Chat 3.4.9	A Cross-Site Scripting vulnerability exists in the web server component due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary HTML and script code.  There is no exploit code required; however, a Proof of Concept exploit has been published.	SCI Photo Chat Server Cross-Site Scripting
<b>High</b>	Sun Microsystems, Inc. <sup>60</sup>  Enterprise Storage Manager 2.1, StorEdge 3310 SCSI Array, 3510 FC Array	A vulnerability exists when a non-root user has been assigned the 'ESMUser' role on the management station, which could let a malicious user obtain superuser privileges.  Patch available at: <a href="https://sunsolve.sun.com/pub-cgi/117367-01.jar">https://sunsolve.sun.com/pub-cgi/117367-01.jar</a>  Currently we are not aware of any exploits for this vulnerability.	Sun Enterprise Storage Manager Privilege Escalation
<b>High</b>	The Miller Group <sup>61</sup>  Centre 0.92, 1.0 1, 1.0	A vulnerability exists in 'modules.php' due to insufficient validation of the location of the user-supplied 'modname' parameter, which could let a remote malicious user execute arbitrary PHP code.  Upgrade available at: <a href="http://www.miller-group.net/">http://www.miller-group.net/</a>  A Proof of Concept exploit has been published.	Centre 'modules.php' Remote PHP Code Execution

<sup>56</sup> Debian Security Advisory, DSA 527-1, July 3, 2004.

<sup>57</sup> Gentoo Linux Security Advisory, GLSA 200406-22, June 30, 2004.

<sup>58</sup> SecurityTracker Alert, 1010614, June 30, 2004.

<sup>59</sup> Secunia Advisory, SA12015, July 6, 2004.

<sup>60</sup> Sun(sm) Alert Notification, 57581, June 18, 2004.

<sup>61</sup> SecurityTracker Alert, 1010634, July 3, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	TildeSlash <sup>62</sup>  Monit 1.0, 1.1, 1.2, 1.3, 1.3.1, 1.4, 1.4.1, 2.0-2.4.3, 3.0-3.2, 4.0, 4.1, 4.1.1, 4.2	A buffer overflow vulnerability exists during authentication handling due to a failure to properly handle user-supplied strings when copying them into finite stack-based buffers, which could let a malicious user execute arbitrary code as the superuser.  Updates available at: <a href="http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz">http://www.tildeslash.com/monit/dist/monit-4.2.1.tar.gz</a>  Exploit script has been published.	TildeSlash Monit Authentication Buffer Overflow
<b>High</b>	Webman <sup>63</sup>  Commerce i-mall.cgi	An input validation vulnerability exists because the 'p' parameter does not properly validate user-supplied input, which could let a remote malicious user execute arbitrary commands.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proof of Concept exploit script has been published.	I-Mall Input Validation
<b>High</b>	William Deich Debian <sup>64</sup>  Debian Linux 3.0, sparc, s/390, ppc, mipsel, mips, m68k, ia-64, 3.0 ia-32, hppa, arm, alpha; William Deich super 3.12, 3.16-3.19	A format string vulnerability exists due to incorrect usage of programming functions designed to take formatted arguments, which could let a remote malicious user execute arbitrary code with superuser privileges.  <b>Debian:</b> <a href="http://security.debian.org/pool/updates/main/s/super/">http://security.debian.org/pool/updates/main/s/super/</a>  Currently we are not aware of any exploits for this vulnerability.	Super Local Format String  CVE Name: CAN-2004-0579
<b>High/Medium</b>  (High if arbitrary code can be executed; and Medium is sensitive information can be obtained, comments deleted, Or journal entries added)	Francisco Burzi <sup>65</sup>  PHP-Nuke 1.0, 2.5, 3.0, 4.0, 4.3, 4.4, 4.4.1 a, 5.0, 5.0.1, 5.1, 5.2 a, 5.2, 5.3.1, 5.4-5.6, 6.0, 6.5, RC1-RC3, BETA1, FINAL, 6.6, 6.7, 6.9, 7.0, FINAL, 7.1-7.3	Multiple vulnerabilities exist: a vulnerability exists because path information can be disclosed in error pages by passing invalid input or accessing scripts directly, which could let a remote malicious user obtain sensitive information; a vulnerability exists in 'modules/Journal/search.php' due to insufficient verification of user-supplied input, which could let a remote malicious user execute arbitrary code; a vulnerability exists because several Journal scripts do not filter HTML code from user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability exists because the 'modules/Journal/commentkill.php' script does not require authentication, which could let a remote malicious user delete comments; and a vulnerability exists in 'modules/Journal/savenew.php' due to insufficient authentication, which could let a remote malicious user add new journal entries.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proofs of Concept exploits have been published.	PHP-Nuke Multiple Vulnerabilities

<sup>62</sup> SecurityFocus, June 21, 2004.

<sup>63</sup> SecurityTracker Alert, 1010609, June 29, 2004.

<sup>64</sup> Debian Security Advisory DSA 522-1, June 19, 2004.

<sup>65</sup> Secunia Advisory, SA11920, June 23, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Medium</b></p> <p>(High if arbitrary code can be executed; and Medium is sensitive information can be obtained)</p>	<p>OSTicket.com<sup>66</sup></p> <p>osTicket STS 1.2</p>	<p>Multiple vulnerabilities exist: a vulnerability exists because attachments that are submitted as part of a support ticket request are stored with a predictable name in a known web location, which could let a remote malicious user obtain sensitive information; a vulnerability exists because users are not required to validate e-mail used to open a ticket via the on-line form, which could let a remote malicious user execute arbitrary code; and a vulnerability exist because file upload size limitations can be bypassed, which could let a remote malicious user execute arbitrary code.</p> <p>Upgrade available at:  <a href="http://www.osticket.com/downloads/osticket_1.2.7.zip">http://www.osticket.com/downloads/osticket_1.2.7.zip</a></p> <p>There is no exploit code required; however, a Proof of Concept exploit has been published.</p>	<p>OSTicket Multiple Vulnerabilities</p>
<p><b>High/Medium</b></p> <p>(Medium if arbitrary code can be executed; and Medium is sensitive information can be obtained)</p>	<p>PowerPortal<sup>67</sup></p> <p>PowerPortal 1.1 b, 1.3 b, 1.3</p>	<p>Multiple vulnerabilities exist: multiple Cross-Site Scripting vulnerabilities exist due to insufficient sanitization of user-supplied data, which could let a remote malicious user execute arbitrary HTML and script code; a Directory Traversal vulnerability exists in the 'modules.php' script, which could let a remote malicious user obtain sensitive information; and an information disclosure vulnerability exists because a remote malicious user can determine the installation path.</p> <p>No workaround or patch available at time of publishing</p> <p>Proofs of Concept exploits have been published.</p>	<p>PowerPortal Multiple Input Validation</p>
<p><b>High/Low</b></p> <p>(High if arbitrary code can be executed; and Low if a DoS)</p>	<p>Carl Harris<sup>68</sup></p> <p>popclient 3.0 b6</p>	<p>An off-by-one buffer overflow vulnerability exists in the 'POP3_readmsg()' function when processing a specially crafted e-mail with an overly long line, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	<p>popclient Off-By-One Overflow</p>

<sup>66</sup> osTicket Security Alert, June 26, 2004.

<sup>67</sup> Secunia Advisory, SA11960, June 29, 2004.

<sup>68</sup> Securiteam, July 1, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p>(High if arbitrary code can be executed; and Low if a DoS)</p>	<p>ISC<sup>69</sup> Fedora<sup>70</sup> Mandrake<sup>71</sup> SuSE<sup>72</sup></p> <p>ISC DHCPD 3.0.1 rc12 &amp; rc13; RedHat Fedora Core2; SuSE Linux 8.0, i386, 8.1, 8.2, 9.0, x86_64, 9.1, Admin-CD for Firewall , Connectivity Server, Database Server, Enterprise Server 8, 7, Firewall on CD, Office Server, SuSE eMail Server III</p>	<p>Several vulnerabilities exist: a buffer overflow vulnerability exists in routines that are responsible for logging hostname options, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and a buffer overflow vulnerability exists on systems that lack a 'vsprintf()' library function (ISC DHCPD defines vsprintf as: #define vsprintf(buf, size, fmt, list) vsprintf (buf, fmt, list) , which could let a remote malicious user cause a Denial of Service or execute arbitrary code.</p> <p>Upgrade available at: <a href="ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.lrc14.tar.gz">ftp://ftp.isc.org/isc/dhcp/dhcp-3.0.lrc14.tar.gz</a> <b>Fedora:</b> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</a> <b>Mandrake:</b> <a href="http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:061">http://www.mandrakesoft.com/security/advisories?name=MDKSA-2004:061</a> <b>SuSE:</b> <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>ISC DHCP Remote Buffer Overflows</p> <p>CVE Names: CAN-2004-0460, CAN-2004-0461</p>
<p><b>High/Low</b></p> <p>(High if arbitrary code can be executed; and Low if a DoS)</p>	<p>linux1394.org<sup>73</sup> Astaro Caldera Conectiva CRUX Debian Devil-Linux Gentoo Mandrake RedHat Slackware SuSE Trustix TurboLinux WOLK</p> <p>Linux kernel 2.4.0-test1-test12, 2.4-2.4.27 -pre2, 2.5.0-2.5.69, 2.6, test1-test11, 2.6.1-2.6.7</p>	<p>An integer overflow vulnerability exists in the 'IEEE 1394 for Linux' Firewire driver, which could let a malicious user cause a Denial of Service or possibly execute arbitrary code.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Linux Kernel IEEE 1394 Integer Overflow</p>

<sup>69</sup> Technical Cyber Security Alert TA04-174A, <http://www.us-cert.gov/cas/techalerts/TA04-174A.html>.

<sup>70</sup> Fedora Update Notification, FEDORA-2004-190, June 23, 2004.

<sup>71</sup> Mandrake Security Advisory, MDKSA-2004:06, June 22, 2004.

<sup>72</sup> SUSE Security Announcement, SuSE-SA:2004:019, June 22, 2004.

<sup>73</sup> Securiteam, June 24, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High/Low</b>  (High if arbitrary code can be executed; and Low if a DoS)	mplayerhq.hu <sup>74</sup>  MPlayer HEAD CVS, 0_92 CVS, 0.9 0rc4, 0.90 rc series, 0.90 pre series, 0.90, 0.91, 0.92, 0.92.1, 1.0 pre4, 1.0 pre3try2, 1.0 pre3, 1.0 pre2, 1.0 pre1	A buffer overflow vulnerability exists in the 'TranslateFilename()' function due to a failure to properly handle user-supplied strings when copying them into finite buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.  No workaround or patch available at time of publishing.  A Proof of Concept exploit has been published.	MPlayer GUI Buffer Overflow
<b>High/Low</b>  (High if arbitrary code can be executed; and Low if a DoS)	Multiple Vendors <sup>75</sup> Astaro Caldera Conectiva CRUS Debian Devil-Linux Gentoo Mandrake RedHat Slackware SuSE TurboLinux Trustix WOLK  Linux kernel 2.4, 2.4.0-test1-test12, 2.4.1-2.4.27 -pre2	Several integer overflow vulnerabilities exists in the 'copyin()' and 'copyin_string()' functions of the Sbus PROM driver, which could let a remote malicious user cause a Denial of Service and possible execute arbitrary code.  No workaround or patch available at time of publishing.  Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Sbus PROM Driver Multiple Integer Overflow
<b>High/Low</b>  (High if arbitrary code can be executed; and Low if a DoS)	RedHat <sup>76</sup>  Linux kernel-2.4.20-8.athlon.rpm, 2.4.20-8.i386.rpm, 2.4.20-8.i586.rpm, 2.4.20-8.i686.rpm, kernel-smp-2.4.20-8.athlon.rpm, kernel-smp-2.4.20-8.i586.rpm , kernel-smp-2.4.20-8.i686.rpm , kernel-source-2.4.20-8.i386.rpm, Linux 8.0, i686, i386	A buffer overflow vulnerability exists in the 'ubsec_keysetup()' function in '/drivers/crypto/bcm/pkey.c,' which could let a malicious user cause a Denial of Service or possibly execute arbitrary code.  No workaround or patch available at time of publishing.  Currently we are not aware of any exploits for this vulnerability.	BCM5820 Linux Driver Buffer Overflow

<sup>74</sup> Bugtraq, June 27, 2004.

<sup>75</sup> SecurityTracker Alert, 1010617, June 30, 2004.

<sup>76</sup> SecurityTracker Alert, 1010575, June 24, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	BEA Systems, Inc. <sup>77</sup>  WebLogic Express 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Express for Win32 7.0, SP1-SP5, 8.1, SP1&SP2, Weblogic Server 7.0, SP1-SP5, 8.1, SP1&SP2, WebLogic Server for Win32 7.0, SP1-SP5, 8.1, SP1&SP2	A vulnerability exists if a '<role-name>' within a '<security-constraint>' has specified a '*' as role name, which could let a remote malicious user obtain unauthorized access.  Patches available at: <a href="ftp://ftpna.beasys.com/pub/releases/security/CR175310_700sp5.jar">ftp://ftpna.beasys.com/pub/releases/security/CR175310_700sp5.jar</a> <a href="ftp://ftpna.beasys.com/pub/releases/security/CR175310_810sp2.jar">ftp://ftpna.beasys.com/pub/releases/security/CR175310_810sp2.jar</a>  There is no exploit code required.	BEA WebLogic Server & WebLogic Express role-name Unauthorized Access
Medium	CGISCRIP.T.NET <sup>78</sup>  csFAQ, 1.0	A vulnerability exists in 'csFAQ.cgi' due to insufficient handling of the 'database' parameter, which could let a remote malicious user obtain sensitive information.  No workaround or patch available at time of publishing.  There is no exploit code required; however, a Proof of Concept exploit has been published.	csFAQ Installation Path Disclosure
Medium	Esearch Gentoo <sup>79</sup>  emerge search tool 0.3.1, 0.4-0.4.2, 0.5-0.5.3, 0.6, 0.6.1	A vulnerability exists in 'eupdatedb' due to a failure to properly handle temporary file creation, which could let a malicious user perform certain actions with elevated privileges.  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200407-01.xml">http://security.gentoo.org/glsa/glsa-200407-01.xml</a>  There is no exploit code required.	Esearch eupdatedb Symbolic Link
Medium	Hewlett Packard Company <sup>80</sup>  HP-UX B.11.11	A vulnerability exists in Object Action Manager (ObAM) when the WebAdmin capability is enabled, which could let a remote malicious user obtain unauthorized access.  <b>Workaround:</b> HP recommends that you disable the ObAM web administration interface using the following steps [quoted]:  Check the /etc/rc.config.d/webadmin file. If the default value ("WEBADMIN=0") has been changed, edit the file to set "WEBADMIN=0," and run the following run the following as root to stop the Apache server if it had been running:  /usr/obam/server/bin/apachectl stop  Currently we are not aware of any exploits for this vulnerability.	HP-UX ObAM WebAdmin Unauthorized Access

<sup>77</sup> BEA Systems Security Advisory, BEA04-64.00, June 28, 2004.

<sup>78</sup> Bugtraq, June 28, 2004.

<sup>79</sup> Gentoo Linux Security Advisory, GLSA 200407-01, July 1, 2004.

<sup>80</sup> HP Software Security Response Team Bulletin, SSRT4758, June 28, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	IBM <sup>81</sup>  Lotus Domino 6.5.0, 6.5.1	A vulnerability exists in the 'setquota' command, which could let a remote malicious user alter their mail storage quota values.  No workaround or patch available at time of publishing.  There is no exploit code required.	IBM Lotus Domino IMAP Quota Changing
Medium	Multiple Vendors Andreas Steffen Gentoo <sup>82</sup> Openswan strongSwan Super FreeS/WAN  Andreas Steffen x509 patch 0.9.39, patch 1.5.4, patch 1.5.5; Gentoo Linux 1.4, rc1-rc3; Openswan Openswan 1.0.4, 1.0.5, 2.1.1, 2.1.2; strongSwan strongSwan 2.1.3; Super FreeS/WAN Super FreeS/WAN 1.99.7 .3	A vulnerability exists due to two authentication errors within the 'verify_x509cert()' function when verifying certificates, which could let a remote malicious user store a fake CA certificate to obtain authentication.  <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200406-20.xml">http://security.gentoo.org/glsa/glsa-200406-20.xml</a> <b>Openswan:</b> <a href="http://www.openswan.org/code/">http://www.openswan.org/code/</a> <b>strongSwan:</b> <a href="http://www.strongswan.org/download.htm">http://www.strongswan.org/download.htm</a>  There is no exploit code required.	FreeS/WAN X.509 Patch Certificate Verification
Medium	Phpmyfamily <sup>83</sup>  phpmyfamily 1.2.4, 1.2.5, 1.3	A vulnerability exists when the 'registers_globals' PHP configuration directive is enabled, which could let a remote malicious user obtain elevated privileges.  Upgrades available at: <a href="http://www.phpmyfamily.net/downloads.php">http://www.phpmyfamily.net/downloads.php</a>  There is no exploit code required.	PHPMyFamily Authentication Bypass
Medium	RSBAC Gentoo <sup>84</sup>  RSBAC 1.2.2, 1.2.3; Gentoo Linux 1.4	Two vulnerabilities exist: a vulnerability exists in the FF, RC, and ACL modules due to a failure to prevent the AUTH module from being switched off, which could let a malicious user obtain elevated privileges; and a vulnerability exists in the 'CREATE' module due to a failure to check mode values, which could let a malicious user obtain elevated privileges.  Patches available at: <a href="http://www.rsbac.org/download/bugfixes/v1.2.3/rsbac-bugfix-v1.2.3-3.diff">http://www.rsbac.org/download/bugfixes/v1.2.3/rsbac-bugfix-v1.2.3-3.diff</a> <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200407-02.xml">http://security.gentoo.org/glsa/glsa-200407-02.xml</a>  Currently we are not aware of any exploits for this vulnerability.	RSBAC Multiple Vulnerabilities

<sup>81</sup> Bugtraq, June 30, 2004.

<sup>82</sup> Gentoo Linux Security Advisory, GLSA 200406-20, June 25, 2004.

<sup>83</sup> Secunia Advisory, SA11944, June 28, 2004.

<sup>84</sup> Gentoo Linux Security Advisory, GLSA 200407-02, July 3, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	rssh.sourceforge.net <sup>85</sup>  rssh 2.0, 2.1	A vulnerability exists in rssh when used with chroot due to improper processing of command line arguments that require expansion, which could let a remote malicious user obtain sensitive information.  Upgrades available at: <a href="http://www.pizzashack.org/rssh/">http://www.pizzashack.org/rssh/</a>  <b>There is no exploit code required.</b>	RSSH Information Disclosure
Medium	Sun Microsystems, Inc. <sup>86, 87</sup>  Patch 115168-03, Patch 112908-12	A vulnerability exists in patches 112908-12 and 115168-03 while logging activity due to a failure to secure sensitive information, which could let a malicious user obtain password information.  Patches available at: <a href="http://sunsolve.sun.com/pub-cgi/115168-04.zip">http://sunsolve.sun.com/pub-cgi/115168-04.zip</a> <a href="http://sunsolve.sun.com/pub-cgi/112908-13.zip">http://sunsolve.sun.com/pub-cgi/112908-13.zip</a>  <b>There is no exploit code required.</b>	Solaris Patches 112908-12 And 115168-03 Clear Text Password Logging
Medium	SWSOft <sup>88</sup>  Confixx Pro 3, Pro 2	An information disclosure vulnerability exists in the backup script when a malicious backup request is submitted, which could let a malicious user obtain sensitive information.  No workaround or patch available at time of publishing.  <b>Currently we are not aware of any exploits for this vulnerability.</b>	WSoft Confixx Backup Script Information Disclosure
Medium	Ulf Betlehem <sup>89</sup>  cplay 1.49	A vulnerability exists because a temporary file (/var/tmp/cplay_control) is created in an unsafe manner, which could let a malicious user obtain elevated privileges.  No workaround or patch available at time of publishing.  <b>Currently we are not aware of any exploits for this vulnerability.</b>	cplay Temporary File Creation
Medium	ZaireWeb Solutions <sup>90</sup>  Newsletter ZWS	A vulnerability exists in the 'admin.php' script due to a design error in the implementation of the authentication system, which could let a remote malicious user bypass the administrative interface authentication.  No workaround or patch available at time of publishing.  <b>A Proof of Concept exploit has been published.</b>	ZaireWeb Solutions Newsletter ZWS Administrative Interface Authentication Bypass

<sup>85</sup> Secunia Advisory, SA11926, June 23, 2004.

<sup>86</sup> Sun(sm) Alert Notification, 57587, June 17, 2004.

<sup>87</sup> VU#523710, <http://www.kb.cert.org/vuls/id/523710>.

<sup>88</sup> SecurityTracker Alert, 1010584, June 25, 2004.

<sup>89</sup> Secunia Advisory, SA11924, June 23, 2004.

<sup>90</sup> Bugtraq, June 24, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p>Medium/Low</p> <p>(Medium if sensitive information can be obtained or elevated privileges; and Low if a DoS)</p>	<p>FreeBSD<sup>91</sup></p> <p>FreeBSD 4.8, 4.9, 4.10, 5.2</p>	<p>A vulnerability exists due an error in the processing of some Linux system calls in binary compatibility mode, which could let a remote malicious user obtain sensitive information, elevated privileges, and potentially cause a Denial of Service.</p> <p>Patches available at:  <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:13/linux4.patch">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:13/linux4.patch</a>  <a href="ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:13/linux4.patch.asc">ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-04:13/linux4.patch.asc</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>FreeBSD Linux Binary Compatibility Memory Access</p> <p>CVE Name: CAN-2004-0602</p>
<p>Medium/Low</p> <p>(Medium is sensitive information can be obtained or unauthorized access can be obtained; and Low if a DoS)</p>	<p>Hewlett Packard Company<sup>92</sup></p> <p>HP-UX B.11.23, B.11.22, B.11.11, B.11.00</p>	<p>Multiple vulnerabilities exist in the Netscape browser, which could let a remote malicious user cause a Denial of Service, obtain sensitive information, or unauthorized access.</p> <p>HP recommends users to remove Netscape and upgrade to Mozilla.  <a href="http://www.hp.com/go/mozilla">http://www.hp.com/go/mozilla</a></p> <p>Currently we are not aware of any exploits for this vulnerability. Vulnerability has appeared in the press and other public media.</p>	<p>HP-UX Netscape Browser Multiple Vulnerabilities</p>
<p>Low</p>	<p>Apache Software Foundation Apple Mandrake<sup>93</sup> Trustix<sup>94</sup></p> <p>Apache 2.0.47-2.0.49</p>	<p>A remote Denial of Service vulnerability exists in the 'ap_get_mime_headers_core()' function due to a failure to handle excessively long HTTP header strings.</p> <p>Patches available at:  <a href="http://www.apache.org/dist/httpd/patches/apply_to_2.0.49/CAN-2004-0493.patch">http://www.apache.org/dist/httpd/patches/apply_to_2.0.49/CAN-2004-0493.patch</a>  <b>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a>  <b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Apache ap_escape_html Remote Denial of Service</p> <p>CVE Name: CAN-2004-0493</p>
<p>Low</p>	<p>FreeBSD<sup>95</sup></p> <p>FreeBSD 4.10 – RELEASE, 5.1 – RELENG, 5.1 - RELEASE/Alpha, 5.1 -RELEASE-p5, 5.1 –RELEASE, 5.1, 5.2.1 - RELEASE</p>	<p>A Denial of Service vulnerability exists when a malicious user submits a specially crafted execve() system call with an unaligned memory address as the second or third argument.</p> <p>No workaround or patch available at time of publishing.</p> <p>Exploit script has been published.</p>	<p>FreeBSD execve() Denial of Service</p>

<sup>91</sup> FreeBSD Security Advisory, FreeBSD-SA-04:13, July 1, 2004.

<sup>92</sup> Hewlett Packard Security Advisory, HPSBUX0202-182, June 30, 2004.

<sup>93</sup> Mandrakelinux Security Update Advisory, MDKSA-2004:064, June 29, 2004.

<sup>94</sup> Trustix Security Advisory, TSL-2004-0038, June 29, 2004.

<sup>95</sup> Bugtraq, June 23, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	gift-fasttrack.berlios.de <sup>96</sup> Gentoo <sup>97</sup>  giFT-FastTrack 0.8.0-0.8.6	A remote Denial of Service vulnerability exists in the HTTP header parser when a malicious user submits malformed HTTP requests.  Upgrades available at: <a href="http://download.berlios.de/gift-fasttrack/giFT-FastTrack-0.8.7.tar.gz">http://download.berlios.de/gift-fasttrack/giFT-FastTrack-0.8.7.tar.gz</a> <b>Gentoo:</b> <a href="http://security.gentoo.org/glsa/glsa-200406-19.xml">http://security.gentoo.org/glsa/glsa-200406-19.xml</a>  <b>There is no exploit code required.</b>	giFT-FastTrack HTTP Header Parser Remote Denial of Service
Low	GNU <sup>98</sup>  Radius 1.1	A remote Denial of Service vulnerability exists when handling SNMP messages that contain invalid Object ID data.  Upgrade available at: <a href="http://ftp.gnu.org/gnu/radius/radius-1.2.tar.gz">http://ftp.gnu.org/gnu/radius/radius-1.2.tar.gz</a>  <b>Currently we are not aware of any exploits for this vulnerability.</b>	GNU Radius SNMP OID Remote Denial of Service  <b>CVE Name:</b> <b>CAN-2004-0576</b>
Low	Hewlett Packard Company <sup>99</sup>  HP-UX B.11.11, B.11.04, B.11.00	A Denial of Service vulnerability exists due to an unspecified error within the HP-UX ARPA Transport.  Patches available at: <a href="http://itrc.hp.com/">http://itrc.hp.com/</a>  <b>Currently we are not aware of any exploits for this vulnerability.</b>	HP-UX ARPA Transport Denial of Service
Low	IBM <sup>100</sup>  Lotus Domino 6.5.1	A remote Denial of Service vulnerability exists when a malicious user's e-mail is opened through the Domino Web Access.  No workaround or patch available at time of publishing.  <b>A Proof of Concept exploit has been published.</b>	IBM Lotus Domino Remote Denial of Service
Low	IBM <sup>101</sup>  WebSphere Caching Proxy Server 5.0 2, Edge server Caching proxy 5.0 2	A Denial of Service vulnerability exists in the Caching Proxy component due to a failure to handle incomplete 'GET' requests, if the 'JunctionRewrite' and 'UseCookie' directives are active.  IBM reportedly plans to release a fixed version (5.0.3). Also, IBM customers with Support Level 2 or 3 can request a patch.  <b>There is no exploit code required; however, a Proof of Concept exploit has been published.</b>	IBM WebSphere Edge Server Component Caching Proxy Denial of Service

<sup>96</sup> Secunia Advisory, SA11941, June 25, 2004.

<sup>97</sup> Gentoo Linux Security Advisory, GLSA 200406-19, June 24, 2004.

<sup>98</sup> Securiteam, June 22, 2004.

<sup>99</sup> HP Software Security Response Team Bulletin, SSRT3552, June 29, 2004.

<sup>100</sup> Bugtraq, June 30, 2004.

<sup>101</sup> CYBSEC Security Advisory, July 2, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Multiple Vendors Fedora <sup>102</sup> SuSE <sup>103</sup>  Linux kernel 2.6, Linux kernel 2.6.1, rc1-rc2, 2.6.2-2.6.5, 2.6.6, rc1, 2.6.7, rc1; S.u.S.E. Linux 8.0, i386, 8.1, 8.2, 9.0, x86_64, 9.1, Linus Admin-CD for Firewall , Linus Connectivity Server, Linux Database Server, Linux Enterprise Server 8, 7, Linux Firewall on CD, Linux Office Server, Office Server, eMail Server 3.1, eMail Server III	A remote Denial of Service vulnerability exists in the IPTables implementation due to a failure to handle certain TCP packet header values.  <b>Fedora:</b> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/</a> <b>SuSE:</b> <a href="ftp://ftp.suse.com/pub/suse/">ftp://ftp.suse.com/pub/suse/</a>  There is no exploit code required.	Linux Kernel IPTables Sign Error Remote Denial of Service
Low	Sun Microsystems, Inc. <sup>104, 105</sup>  Solaris 7.0, 7.0 _x86, 8.0, 8.0 _x86, 9.0, 9.0_x86 Update 2, 9.0_x86	A Denial of Service vulnerability exists in the Basic Security Module (BSM) when configured to audit either the administrative audit class 'ad' or the system-wide administration audit class 'as.'  Patches available at: <a href="http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57497">http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57497</a>  Currently we are not aware of any exploits for this vulnerability.	Sun Solaris Basic Security Module Auditing Denial of Service
Low	Sun Mircoystems, Inc. <sup>106</sup>  Sun JRE (Linux Production Release) 1.4.1_01-1.4.1_03, 1.4.1, 1.4.2_01 -1.4.2_04, 1.4.2, JRE (Solaris Production Release) 1.4.1_01-1.4.1_03, 1.4.1, 1.4.2_01 -1.4.2_04, 1.4.2, JRE (Windows Production Release) 1.4.1_01-1.4.1_03, 1.4.1_07, 1.4.1, 1.4.2_01-1.4.2_04, 1.4.2	A Denial of Service vulnerability exists in the Sun Java Runtime Environment Font object due to a failure to handle exceptional conditions when processing font objects.  No workaround or patch available at time of publishing.  A Proof of Concept exploit script has been published.	Sun Java Runtime Environment Font Object Denial of Service

<sup>102</sup> Fedora Update Notification, FEDORA-2004-202, June 30, 2004.

<sup>103</sup> SUSE Security Announcement, SUSE-SA:2004:020, July 2, 2004.

<sup>104</sup> Sun(sm) Alert Notification, 57497, June 22, 2004.

<sup>105</sup> VU#901582, <http://www.kb.cert.org/vuls/id/901582>.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	MIT <sup>107,108</sup> <i>Debian</i> <sup>109</sup> <i>Fedora</i> <sup>110</sup> <i>Gentoo</i> <sup>111</sup> Immunix Mandrake <sup>112</sup> OpenBSD <i>RedHat</i> <sup>113</sup> <i>SGI</i> <sup>114</sup> <i>Sun</i> <sup>115</sup> Tinysofa <sup>116</sup> Trustix <sup>117</sup>  Kerberos 5 1.0, 1.0.6, 1.0.8, 1.1, 1.1.1, 1.2.1-1.2.7, 1.3 -alpha1, 5.0 - 1.3.3, 5.0 - 1.2beta1&2, 5.0 - 1.1.1, 5.0 -1.1, 5.0 - 1.0.x; tinysofa enterprise server 1.0 -U1, 1.0  <i>Gentoo issues advisory</i>	<p>Multiple buffer overflow vulnerabilities exist due to boundary errors in the 'krb5_aname_to_localname()' library function during conversion of Kerberos principal names into local account names, which could let a remote malicious user execute arbitrary code with root privileges.</p> <p>Patch available at:  <a href="http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt">http://web.mit.edu/kerberos/advisories/2004-001-an_to_ln_patch.txt</a>  <b>Mandrake:</b>  <a href="http://www.mandrakesoft.com/security/advisories">http://www.mandrakesoft.com/security/advisories</a>  <b>Tinysofa:</b>  <a href="http://www.tinysofa.org/support/errata/2004/009.html">http://www.tinysofa.org/support/errata/2004/009.html</a>  <b>Trustix:</b>  <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p> <p><b>Debian:</b>  <a href="http://security.debian.org/pool/updates/main/k/krb5/">http://security.debian.org/pool/updates/main/k/krb5/</a>  <b>Fedora:</b>  <a href="http://securityfocus.com/advisories/6817">http://securityfocus.com/advisories/6817</a>  <b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2004-236.html">http://rhn.redhat.com/errata/RHSA-2004-236.html</a>  <b>SGI:</b>  <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/3/">ftp://patches.sgi.com/support/free/security/patches/ProPack/3/</a>  <b>Sun:</b>  <a href="http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57580">http://sunsolve.sun.com/pub-cgi/retrieve.pl?doc=fsalert%2F57580</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200406-21.xml">http://security.gentoo.org/glsa/glsa-200406-21.xml</a></p>	Kerberos 5 'krb5_aname_to_localname' Multiple Buffer Overflows  <b>CVE Name:</b> <b>CAN-2004-0523</b>
<b>High</b>	rlrp Debian <sup>118</sup>  rlrp 2.0 1-2.0.4, 2.0  <i>Exploit script has been published</i> <sup>119</sup>	<p>Multiple vulnerabilities exist: a format string vulnerability exists in the 'msg()' function due to a syslog(3) call made without the proper format string specifier, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the 'msg()' function due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.</p> <p><b>Debian:</b>  <a href="http://security.debian.org/pool/updates/main/r/rlrp/">http://security.debian.org/pool/updates/main/r/rlrp/</a></p> <p><i>Exploit script has been published.</i></p>	Rlrp Multiple Vulnerabilities  <b>CVE Names:</b> <b>CAN-2004-0393,</b> <b>CAN-2004-0454</b>

<sup>106</sup> SecurityFocus, June 28, 2004.

<sup>107</sup> MIT krb5 Security Advisory 2004-001, June 3, 2004.

<sup>108</sup> TA04-147A, <http://www.kb.cert.org/vuls/id/686862>.

<sup>109</sup> Debian Security Advisory DSA 520-1, June 16, 2004.

<sup>110</sup> Fedora Update Notification, FEDORA-2004-149 & 150, June 4, 2004.

<sup>111</sup> Gentoo Linux Security Advisory, GLSA 200406-21, June 29, 2004.

<sup>112</sup> Mandrakelinux Security Update Advisory, MDKSA-2004:056, June 3, 2004.

<sup>113</sup> RedHat Security Advisory, RHSA-2004:236-14, June 9, 2004.

<sup>114</sup> SGI Security Advisories, 20040604-01-U & 20040605-01-U, June 21, 2004.

<sup>115</sup> Sun(sm) Alert Notification, 57580, June 10, 2004.

<sup>116</sup> Tinasofa Security Advisory, TSSA-2004-009, June 2, 2004.

<sup>117</sup> Trustix Security Advisory, TSLSA-2004-0032, June 2, 2004.

<sup>118</sup> Debian Security Advisory, DSA 524-1, June 19, 2004.

<sup>119</sup> SecurityFocus, June 24, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	SquirrelMail Development Team <sup>120</sup> <i>Fedora</i> <sup>121</sup> <i>Gentoo</i> <sup>122</sup> <i>RedHat</i> <sup>123</sup> <i>SGI</i> <sup>124</sup>  SquirrelMail 1.0.4, 1.0.5, 1.2.0-1.2.11, 1.4-1.4.2  <i>More vendors issue advisories</i>	A vulnerability exists due to input validation errors, which could let a remote malicious user execute arbitrary HTML and script code.  <b>Upgrades available at:</b> <a href="http://sourceforge.net/project/showfiles.php?group_id=311&amp;package_id=334&amp;release_id=237332">http://sourceforge.net/project/showfiles.php?group_id=311&amp;package_id=334&amp;release_id=237332</a>  <b>There is no exploit code required.</b>  <i>Fedora:</i> <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</a> <i>RedHat:</i> <a href="http://rhn.redhat.com/errata/RHSA-2004-240.html">http://rhn.redhat.com/errata/RHSA-2004-240.html</a> <i>SGI:</i> <a href="ftp://patches.sgi.com/support/free/security/">ftp://patches.sgi.com/support/free/security/</a>	SquirrelMail SQL Injection  <b>CVE Name:</b> <b>CAN-2004-0521</b>
<b>High/ Medium</b>  <b>(Medium if sensitive information can be obtained or corrupted)</b>	Invision Power Services <sup>125</sup>  Invision Board 1.3.1 Final  <i>Upgrade now available</i> <sup>126</sup>	An input validation vulnerability exists in 'ssi.php' due to insufficient validation or user-supplied input, which could let a remote malicious user obtain/modify sensitive information or execute arbitrary commands.  <b>Upgrade available at:</b> <a href="http://forums.invisionpower.com/index.php?act=Attach&amp;type=post&amp;id=1096">http://forums.invisionpower.com/index.php?act=Attach&amp;type=post&amp;id=1096</a>  <b>There is no exploit code required; however, a Proof of Concept exploit has been published.</b>	Invision Power Board Input Validation

<sup>120</sup> Secunia Advisory, SA11685, May 21, 2004.

<sup>121</sup> Fedora Update Notification, FEDORA-2004-160, June 9, 2004.

<sup>122</sup> Gentoo Linux Security Advisories, GLSA 200405-16 & 16:02, May 21 & 25, 2004.

<sup>123</sup> RedHat Security Advisory, RHSA-2004:240-06, June 14, 2004.

<sup>124</sup> SGI Security Advisory, 20040604-01-U, June 21, 2004.

<sup>125</sup> SecurityTracker Alert, 1010448, June 9, 2004.

<sup>126</sup> SecurityFocus, June 30, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Medium</b></p> <p><b>(High if arbitrary code can be executed)</b></p>	<p>Multiple Vendors</p> <p><i>Conectiva</i><sup>127</sup></p> <p>Clearswift</p> <p><i>Debian</i><sup>128</sup></p> <p><i>F-Secure</i><sup>129</sup></p> <p><i>Fedora</i><sup>130</sup></p> <p><i>Gentoo</i><sup>131</sup></p> <p>Mr. S.K.</p> <p>RARLAB</p> <p>RedHat<sup>132</sup></p> <p><i>SGI</i><sup>133</sup></p> <p>Slackware<sup>134</sup></p> <p>Stalker</p> <p>WinZip</p> <p>Mr. S.K. LHA 1.14, 1.15, 1.17; RARLAB WinRAR 3.20; RedHat lha-1.14i-9.i386.rpm; WinZip 9.0; Stalker CGPMcAfee 3.2</p> <p><i>SGI issues advisory</i></p>	<p>Multiple vulnerabilities exist: two buffer overflow vulnerabilities exist when creating a carefully crafted LHA archive, which could let a remote malicious user execute arbitrary code; and several Directory Traversal vulnerabilities exist, which could let a remote malicious user corrupt/overwrite files in the context of the user who is running the affected LHA utility.</p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/i386/lha-1.14i-9.1.i386.rpm">ftp://updates.redhat.com/9/en/os/i386/lha-1.14i-9.1.i386.rpm</a></p> <p><b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><b>Proofs of Concept exploits have been published.</b></p> <p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p><b>Debian:</b>  <a href="http://security.debian.org/pool/updates/non-free/l/lha/">http://security.debian.org/pool/updates/non-free/l/lha/</a></p> <p><b>F-Secure:</b>  <a href="http://www.f-secure.com/security/fsc-2004-1.shtml">http://www.f-secure.com/security/fsc-2004-1.shtml</a></p> <p><b>Fedora:</b>  <a href="http://www.redhat.com/archives/fedora-announce-list/2004-May/msg00005.html">http://www.redhat.com/archives/fedora-announce-list/2004-May/msg00005.html</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200405-02.xml">http://security.gentoo.org/glsa/glsa-200405-02.xml</a></p> <p><b>SGI:</b>  <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p>	<p>Multiple LHA Buffer Overflow/Directory Traversal Vulnerabilities</p> <p><b>CVE Names:</b>  <b>CAN-2004-0234,</b>  <b>CAN-2004-0235</b></p>

<sup>127</sup> Conectiva Linux Security Announcement, CLA-2004:840, May 7, 2004.

<sup>128</sup> Debian Security Advisory DSA 515-1, June 5, 2004.

<sup>129</sup> F-Secure Security Bulletin, FSC-2004-1, May 26, 2004.

<sup>130</sup> Fedora Update Notification, FEDORA-2004-119, May 11, 2004.

<sup>131</sup> Gentoo Linux Security Advisory, GLSA 200405-02, May 9, 2004.

<sup>132</sup> Red Hat Security Advisory, RHSA-2004:179-01, April 30, 2004.

<sup>133</sup> SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004.

<sup>134</sup> Slackware Security Advisory, SSA:2004-125-01, May 5, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(High if arbitrary code can be executed)</b></p>	<p>Apache Software Foundation<sup>135</sup></p> <p><i>Gentoo</i><sup>136</sup></p> <p><i>Mandrake</i><sup>137</sup></p> <p><i>OpenBSD</i></p> <p><i>OpenPKG</i><sup>138</sup></p> <p><i>RedHat</i><sup>139</sup></p> <p><i>SGI</i><sup>140</sup></p> <p><i>Tinysofa</i><sup>141</sup></p> <p><i>Trustix</i><sup>142</sup></p> <p>Apache 1.3-2.0.49</p> <p><i>More vendor advisories issued</i></p>	<p>A stack-based buffer overflow has been reported in the Apache mod_ssl module. This issue would most likely result in a Denial of Service if triggered, but could theoretically allow for execution of arbitrary code. The issue is not believed to be exploitable to execute arbitrary code on x86 architectures, though this may not be the case with other architectures.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p> <p>Patch available at:</p> <p><a href="http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&amp;r2=1.106">http://cvs.apache.org/viewcvs.cgi/httpd-2.0/modules/ssl/ssl_engine_kernel.c?r1=1.105&amp;r2=1.106</a></p> <p><u>Mandrake:</u> <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a></p> <p><u>OpenPKG:</u> <a href="ftp://ftp.openpkg.org">ftp://ftp.openpkg.org</a></p> <p><u>Tinysofa:</u> <a href="http://www.tinysofa.org/support/errata/2004/008.html">http://www.tinysofa.org/support/errata/2004/008.html</a></p> <p><u>Trustix:</u> <a href="http://http.trustix.org/pub/trustix/updates/">http://http.trustix.org/pub/trustix/updates/</a></p> <p><u>Gentoo:</u> <a href="http://security.gentoo.org/glsa/glsa-200406-05.xml">http://security.gentoo.org/glsa/glsa-200406-05.xml</a></p> <p><u>OpenBSD:</u> <a href="http://www.openbsd.org/errata.html">http://www.openbsd.org/errata.html</a></p> <p><u>SGI:</u> <a href="ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/">ftp://patches.sgi.com/support/free/security/patches/ProPack/2.4/</a></p>	<p>Apache Mod_SSL SSL_Util_UUEn code_Binary Stack Buffer Overflow Vulnerability</p> <p><b>CVE Name:</b> <b>CAN-2004-0488</b></p>

<sup>135</sup> Security Focus, May 17, 2004

<sup>136</sup> Gentoo Linux Security Advisory, GLSA 200406-05, June 9, 2004.

<sup>137</sup> Mandrakelinux Security Update Advisories, MDKSA-2004:054 & 055, June 1, 2004.

<sup>138</sup> OpenPKG Security Advisory, OpenPKG-SA-2004.026, May 27, 2004.

<sup>139</sup> RedHat Security Advisory, RHSA-2004:342-10, July 6, 2004.

<sup>140</sup> SGI Security Advisory, 20040605-01-U, June 21, 2004.

<sup>141</sup> Tinysofa Security Advisory, TSSA-2004-008, June 2, 2004.

<sup>142</sup> Trustix Security Advisory, TSLSA-2004-0031, June 2, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(Low if a DoS)</b></p>	<p>Apache Software Foundation<sup>143</sup></p> <p>Conectiva</p> <p><i>Gentoo</i><sup>144</sup></p> <p>HP</p> <p>Immunix</p> <p><i>Mandrake</i><sup>145</sup></p> <p>OpenBSD</p> <p>OpenPKG<sup>146</sup></p> <p>RedHat</p> <p><i>SGI</i><sup>147</sup></p> <p>Trustix</p> <p>Apache 1.3.26-1.3.29, 1.3.31;</p> <p>OpenBSD – current, 3.4, 3.5</p> <p><i>More vendor advisories issued</i></p>	<p>A buffer overflow vulnerability exists in Apache mod_proxy when a ‘ContentLength:’ header is submitted that contains a large negative value, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code.</p> <p>Patches available at:</p> <p><a href="http://marc.theaimsgroup.com/?l=apache-httpd-dev&amp;m=108687304202140&amp;q=p3">http://marc.theaimsgroup.com/?l=apache-httpd-dev&amp;m=108687304202140&amp;q=p3</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>OpenPKG:</b> <a href="ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm">ftp://ftp.openpkg.org/release/2.0/UPD/apache-1.3.29-2.0.3.src.rpm</a></p> <p><b>Currently we are not aware of any exploits for this vulnerability.</b></p> <p><i>Gentoo:</i> <a href="http://security.gentoo.org/glsa/glsa-200406-16.xml">http://security.gentoo.org/glsa/glsa-200406-16.xml</a></p> <p><i>Mandrake:</i> <a href="http://www.mandrakesoft.com/security/advisories">http://www.mandrakesoft.com/security/advisories</a></p> <p><i>SGI:</i> <a href="ftp://patches.sgi.com/support/free/security/">ftp://patches.sgi.com/support/free/security/</a></p>	<p>Apache Mod_Proxy Remote Buffer Overflow</p> <p><b>CVE Name:</b> <b>CAN-2004-0492</b></p>

<sup>143</sup> SecurityTracker Alert, 1010462, June 10, 2004.

<sup>144</sup> Gentoo Linux Security Advisory, GLSA 200406-16, June 22, 2004.

<sup>145</sup> Mandrakelinux Security Update Advisory , MDKSA-2004:065, June 29, 2004.

<sup>146</sup> OpenPKG Security Advisory, OpenPKG-SA-2004.029, June 11, 2004.

<sup>147</sup> SGI Security Advisory , 20040605-01-U, June 21, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(Low if a DoS)</b></p>	<p>Epic Games<sup>148</sup></p> <p>ARUSH Devastation 390.0; DreamForge TNN; Outdoors Pro Hunter; Epic Games Unreal Engine 436, 433, 226f, Unreal Tournament 451b, 2003 2225 win32, 2225 macOS, 2199 win32, 2199 macOS, 2199 linux, 2004 win32, macOS; nfogrames TacticalOps 3.4 Infogrames X-com Enforcer; Ion Storm DeusEx 1.112 fm; Nerf Arena Blast Nerf Arena Blast 1.2; Rage Software Mobile Forces 20000.0; Robert Jordan Wheel of Time 333.0 b; Running With Scissors Postal 2 1337</p> <p><i>Exploit script published<sup>149</sup></i></p>	<p>A buffer overflow vulnerability exists when a specially crafted ‘Secure’ query is submitted via UDP with a long ‘query’ value, which could let a remote malicious user cause a Denial of Service and execute arbitrary code.</p> <p>Patches available at:: Unreal Tournament 2004 win32 <a href="http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120">http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120</a> Epic Games Unreal Tournament 2004 macOS: <a href="http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120">http://www.atari-webcenter.com/friends/?module=friends&amp;action=viewDownloadPage&amp;id=120</a></p> <p><i>Exploit script has been published.</i></p>	<p>Epic Games Unreal Engine ‘Secure’ Query Buffer Overflow</p>

<sup>148</sup> SecurityTracker Alert, 1010535, June 18, 2004.

<sup>149</sup> SecurityFocus, June 23, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(High if arbitrary code can be executed; and Low if a DoS)</b></p>	<p>LBL<sup>150</sup>,  <i>Debian</i><sup>151</sup>  <i>Mandrake</i><sup>152</sup>  <i>OpenPKG</i><sup>153</sup>  Trustix<sup>154</sup>  <i>SGI</i><sup>155</sup>  <i>Slackware</i><sup>156</sup></p> <p>tcpdump 3.4 a6, 3.4, 3.5 alpha, 3.5, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1</p> <p><i>SGI issues advisory</i></p>	<p>Two vulnerabilities exist: a buffer overflow vulnerability exists in 'print-isakmp.c' due to insufficient validation of user-supplied input in ISAKMP packets, which could let a remote malicious user cause a Denial of Service and possibly allow the execution of arbitrary code; and a vulnerability exists when a remote malicious user submits an ISAKMP Identification payload with a specially crafted payload length value that is less than eight bytes.</p> <p>Upgrades available at:  <a href="http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz">http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz</a>  <b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>An exploit script has been published for the ISAKMP Identification Payload vulnerability</b></p> <p><i>Debian:</i>  <a href="http://security.debian.org/pool/updates/main/t/tcpdump">http://security.debian.org/pool/updates/main/t/tcpdump</a>  <i>Mandrake:</i>  <a href="Http://www.mandrakesecure.net/en/advisories/">Http://www.mandrakesecure.net/en/advisories/</a>  <i>OpenPKG:</i>  <a href="ftp://ftp.openpkg.org/release/">ftp://ftp.openpkg.org/release/</a>  <i>Slackware:</i>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><i>SGI:</i>  <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p>	<p>TCPDump ISAKMP Buffer Overflow &amp; ISAKMP Identification Payload Integer Underflow</p> <p><b>CVE Names:</b>  <b>CAN-2004-0183,</b>  <b>CAN-2004-0184</b></p>

<sup>150</sup> Rapid7, Inc. Security Advisory, R7-0017, March 30, 2004.

<sup>151</sup> Debian Security Advisory, DSA 478-1, April 6, 2004.

<sup>152</sup> Mandrakelinux Security Update Advisory, MDKSA-2004:030, April 15, 2004.

<sup>153</sup> OpenPKG Security Advisory, OpenPKG-SA-2004.010, April 7, 2004.

<sup>154</sup> Trustix Secure Linux Security Advisory, TSLSA-2004-0015, March 30, 2004.

<sup>155</sup> SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004.

<sup>156</sup> Slackware Security Advisory, SSA:2004-108-01, April 17, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/ Low</b></p> <p><b>(High if arbitrary code can be executed)</b></p>	<p>LBL<sup>157</sup>  <i>Debian</i><sup>158</sup>  <i>Mandrake</i><sup>159</sup>  <i>OpenPKG</i><sup>160</sup>  <i>SGI</i><sup>161</sup>  <i>Slackware</i><sup>162</sup>  Trustix<sup>163</sup></p> <p>tcpdump 3.4 a6, 3.4, 3.5 alpha, 3.5, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1</p> <p><i>SGI issues advisory</i></p>	<p>Two vulnerabilities exist: a buffer overflow vulnerability exists in 'print-isakmp.c' due to insufficient validation of user-supplied input in ISAKMP packets, which could let a remote malicious user cause a Denial of Service and possibly allow the execution of arbitrary code; and a vulnerability exists when a remote malicious user submits an ISAKMP Identification payload with a specially crafted payload length value that is less than eight bytes.</p> <p>Upgrades available at:  <a href="http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz">http://www.tcpdump.org/release/tcpdump-3.8.3.tar.gz</a>  <b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>An exploit script has been published for the ISAKMP Identification Payload vulnerability</b></p> <p><i>Debian:</i>  <a href="http://security.debian.org/pool/updates/main/t/tcpdump">http://security.debian.org/pool/updates/main/t/tcpdump</a>  <i>Mandrake:</i>  <a href="Http://www.mandrakesecure.net/en/advisories/">Http://www.mandrakesecure.net/en/advisories/</a>  <i>OpenPKG:</i>  <a href="ftp://ftp.openpkg.org/release/">ftp://ftp.openpkg.org/release/</a>  <i>Slackware:</i>  <a href="ftp://ftp.slackware.com/pub/slackware/">ftp://ftp.slackware.com/pub/slackware/</a></p> <p><i>SGI:</i>  <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p>	<p>TCPDump ISAKMP Buffer Overflow &amp; ISAKMP Identification Payload Integer Underflow</p> <p><b>CVE Names:</b>  <b>CAN-2004-0183,</b>  <b>CAN-2004-0184</b></p>

<sup>157</sup> Rapid7, Inc. Security Advisory, R7-0017, March 30, 2004.

<sup>158</sup> Debian Security Advisory, DSA 478-1, April 6, 2004.

<sup>159</sup> Mandrakelinux Security Update Advisory, MDKSA-2004:030, April 15, 2004.

<sup>160</sup> OpenPKG Security Advisory, OpenPKG-SA-2004.010, April 7, 2004.

<sup>161</sup> SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004.

<sup>162</sup> Slackware Security Advisory, SSA:2004-108-01, April 17, 2004.

<sup>163</sup> Trustix Secure Linux Security Advisory, TSLSA-2004-0015, March 30, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<p><b>High/Low</b></p> <p><b>(High if root privileges can be obtained; and Low if a DoS)</b></p>	<p>Multiple Vendors            Fedora<sup>164</sup>            Mandrake<sup>165</sup>            Slackware<sup>166</sup>            RedHat<sup>167</sup>            SGI<sup>168</sup></p> <p>Slackware Linux – current, 9.1;            utempter utempter 0.5.2, 0.5.3</p> <p><i>SGI issues advisory</i></p>	<p>Multiple vulnerabilities exist: a vulnerability exists due to an input validation error that causes the application to exit improperly, which could let a malicious user obtain root privileges; and a vulnerability exists due to a failure to validate buffer boundaries, which could let a malicious user cause a Denial of Service.</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>Mandrake:</b>  <a href="http://www.mandrakesecure.net/en/ftp.php">http://www.mandrakesecure.net/en/ftp.php</a></p> <p><b>Slackware:</b>  <a href="ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/l/utempter-1.1.1-i486-1.tgz">ftp://ftp.slackware.com/pub/slackware/slackware-current/slackware/l/utempter-1.1.1-i486-1.tgz</a></p> <p><i>A Proof of Concept exploit has been published.</i></p> <p><b>RedHat:</b>  <a href="ftp://updates.redhat.com/9/en/os/SRPMS/utempter-0.5.5-2.RHL9.0.src.rpm">ftp://updates.redhat.com/9/en/os/SRPMS/utempter-0.5.5-2.RHL9.0.src.rpm</a></p> <p><b>SGI:</b>  <a href="http://www.sgi.com/support/security/">http://www.sgi.com/support/security/</a></p>	<p>UTempter            Multiple Local Vulnerabilities</p> <p><b>CVE Name:</b>  <b>CAN-2004-0233</b></p>
<p><b>Medium</b></p>	<p>Multiple Vendors            Araro            Conectiva<sup>169</sup>            Debian            Devil-Linux            Gentoo<sup>170</sup>            Mandrake            RedHat<sup>171</sup>            Slackware            SuSE            TurboLinux            Trustix<sup>172</sup></p> <p>Linux kernel            2.4.18, 2.4.19,            2.4.21-2.4.26,            2.6-2.6.7</p> <p><i>More vendor advisories issued</i></p>	<p>Vulnerabilities exist in various drivers (aironet, asus_acpi, dectnet, mpu401, msnd, and pss) for the Linux kernel, which could let a malicious user obtain sensitive information or elevated privileges.</p> <p>Update available at:  <a href="http://www.kernel.org/">http://www.kernel.org/</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2004-255.html">http://rhn.redhat.com/errata/RHSA-2004-255.html</a></p> <p><b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>Currently we are not aware of any exploits for this vulnerability.</b></p> <p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200407-02.xml">http://security.gentoo.org/glsa/glsa-200407-02.xml</a></p>	<p>Linux Kernel            Multiple Device Drivers</p> <p><b>CVE Name:</b>  <b>CAN-2004-0495</b></p>

<sup>164</sup> Fedora Update Notification, FEDORA-2004-108, April 21, 2004.

<sup>165</sup> Mandrakelinux Security Update Advisory, MDKSA-2004:031-1, April 21, 2004.

<sup>166</sup> Slackware Security Advisory, SSA:2004-110-01, April 19, 2004.

<sup>167</sup> Red Hat Security Advisory, RHSA-2004:175-01, April 30, 2004.

<sup>168</sup> SGI Security Advisories, 20040602-01-U & 20040603-01-U, June 21, 2004.

<sup>169</sup> Conectiva Linux Security Announcement, CLA-2004:845, June 22, 2004.

<sup>170</sup> Gentoo Linux Security Advisory, GLSA 200407-02, July 3, 2004.

<sup>171</sup> RedHat Security Advisory, RHSA-2004:255-10, June 17, 2004.

<sup>172</sup> Trustix Secure Linux Security Advisory, TSLSA-2004-0035, June 18, 2004.

Risk*	Vendor & Software Name	Unix Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>Low</b>	<p>Multiple Vendors<sup>173</sup></p> <p>Astaro <i>Conectiva</i><sup>174</sup> CRUX Debian Devil-Linux EnGarde<sup>175</sup> Fedora<sup>176</sup> <i>Gentoo</i><sup>177</sup> Mandrake RedHat<sup>178</sup> Slackware<sup>179</sup> SuSE<sup>180</sup> Trustix<sup>181</sup> TurboLinux<sup>182</sup> Wolk</p> <p>EnGarde Secure Community 2.0, Secure Professional 1.5; Linux kernel 2.4.18, 2.4.20-2.4.22, 2.4.25, 2.4.26, 2.6.5, 2.6.6 rc1, 2.6.6, 2.6.7 rc1</p> <p><i>More vendor advisories issued</i></p>	<p>A Denial of Service vulnerability exists in the ‘__clear_fpu()’ function in 'asm-i386/i387.h.'</p> <p><b>Patches available at:</b>  <a href="http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.7.tar.bz2">http://www.kernel.org/pub/linux/kernel/v2.6/linux-2.6.7.tar.bz2</a>  <a href="http://linuxreviews.org/news/2004-06-11_kernel_crash/signal.c.2.4.20.patch.tx">http://linuxreviews.org/news/2004-06-11_kernel_crash/signal.c.2.4.20.patch.tx</a></p> <p><b>Engarde:</b>  <a href="http://infocenter.guardiandigital.com/advisories/">http://infocenter.guardiandigital.com/advisories/</a></p> <p><b>Fedora:</b>  <a href="http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/">http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/</a></p> <p><b>RedHat:</b>  <a href="http://rhn.redhat.com/errata/RHSA-2004-255.html">http://rhn.redhat.com/errata/RHSA-2004-255.html</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/">ftp://ftp.suse.com/pub/suse/</a></p> <p><b>Trustix:</b>  <a href="ftp://ftp.trustix.org/pub/trustix/updates/">ftp://ftp.trustix.org/pub/trustix/updates/</a></p> <p><b>TurboLinux:</b>  <a href="ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/">ftp://ftp.turbolinux.com/pub/TurboLinux/TurboLinux/ia32/</a></p> <p><b>Exploit scripts have been published.</b></p> <p><b>Conectiva:</b>  <a href="ftp://atualizacoes.conectiva.com.br/">ftp://atualizacoes.conectiva.com.br/</a></p> <p><b>Gentoo:</b>  <a href="http://security.gentoo.org/glsa/glsa-200407-02.xml">http://security.gentoo.org/glsa/glsa-200407-02.xml</a></p>	<p>Linux Kernel Assembler Inline Function Denial of Service</p> <p><b>CVE Name:</b> <b>CAN-2004-0554</b></p>

<sup>173</sup> VU#973654, <http://www.kb.cert.org/vuls/id/973654>.

<sup>174</sup> Conectiva Linux Security Announcement, CLA-2004:845, June 22, 2004.

<sup>175</sup> Guardian Digital Security Advisory, ESA-20040621-005, June 21, 2004.

<sup>176</sup> Fedora Update Notification, FEDORA-2004-171, June 14, 2004.

<sup>177</sup> Gentoo Linux Security Advisory, GLSA 200407-02, July 3, 2004.

<sup>178</sup> RedHat Security Advisory, RHSA-2004:255-10, June 17, 2004.

<sup>179</sup> Slackware Security Advisory, SSA:2004-167-01, June 15, 2004.

<sup>180</sup> SUSE Security Announcement, SuSE-SA:2004:017, June 16, 2004.

<sup>181</sup> Trustix Security Advisory, TSLSA-2004-0034, June 16, 2004.

<sup>182</sup> Turbolinux Security Advisory, TLSA-2004-18, June 18, 2004.

## *Multiple/Other Operating Systems*

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
<b>High</b>	Asterisk <sup>183</sup>  Asterisk 0.7 .0-0.7.2	Multiple format string vulnerabilities exist in the logging functions, which could let a remote malicious user execute arbitrary code.  Upgrades available at: <a href="ftp://ftp.asterisk.org/pub/telephony/asterisk/asterisk-0.9.0.tar.gz">ftp://ftp.asterisk.org/pub/telephony/asterisk/asterisk-0.9.0.tar.gz</a>  <b>A Proof of Concept exploit has been published.</b>	Asterisk PBX Multiple Logging Format String Vulnerabilities
<b>High</b>	D-Link <sup>184</sup>  DI-614+ 2.0 f, 2.0 3g, 2.0 3, 2.0, 2.10, 2.18, DI-704 2.56 b6, 2.56 b5, 2.60 b2	A vulnerability exists in the 'HOSTNAME' field due to improper validation of user-supplied input in DHCP messages, which could let a remote malicious user execute arbitrary HTML code.  No workaround or patch available at time of publishing.  <b>There is no exploit code required; however, a Proof of Concept exploit has been published.</b>	D-Link 'HOSTNAME' Input Validation
<b>High</b>	WebSoft <sup>185</sup>  HelpDesk PRO 2.0	A vulnerability exists in the login page due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary code.  Contact the vendor for a patch at: <a href="http://www.websoft.it/">www.websoft.it/</a>  <b>There is no exploit code required.</b>	WebSoft HelpDesk PRO Input Validation
<b>High</b>	WebSoft <sup>186</sup>  Infinity WEB 1.0	A vulnerability exists in the login page due to insufficient sanitization of user-supplied URI input, which could let a remote malicious user execute arbitrary code.  Contact the vendor for a patch at: <a href="http://www.websoft.it/">www.websoft.it/</a>  <b>There is no exploit code required.</b>	WebSoft Infinity WEB Input Validation
<b>Medium</b>	British Telecom <sup>187</sup>  Voyager 2000 Wireless ADSL Router	An information disclosure vulnerability exists in 'public' SNMP MIB community strings, which could let a remote malicious user obtain sensitive information pertaining to the internal protected network.  No workaround or patch available at time of publishing.  <b>A Proof of Concept exploit has been published.</b>	BT Voyager 2000 Wireless ADSL Router Password Disclosure
<b>Medium</b>	kyberdigi labs <sup>188</sup>  php -exec-dir 4.3.2-4.3.7	An input validation vulnerability exists in the 'hp-exec-dir' patch, which could let a malicious user bypass security restrictions.  No workaround or patch available at time of publishing.  <b>There is no exploit code required.</b>	php -exec-dir Patch Security Restrictions Bypass

<sup>183</sup> Zone-h Security Advisory , ZH2004-12SA, June 25, 2004.

<sup>184</sup> SecurityTracker Alert, 1010562, June 22, 2004.

<sup>185</sup> Zone-H Security Team Advisory, ZH2004-10SA, June 26, 2004.

<sup>186</sup> Zone-H Security Team Advisory, ZH2004-14SA, June 27, 2004.

<sup>187</sup> Securiteam, June 22, 2004.

<sup>188</sup> Secunia Advisory, SA11928, June 24, 2004.

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Medium	nCiper <sup>189</sup> netHSM 2.0, 2.1	<p>A vulnerability exists because passphrases that are entered via the netHSM front panel either using the built in thumbwheel or using a directly attached keyboard, are logged improperly, which could let a remote malicious user obtain sensitive information.</p> <p>Upgrade and workaround information available at:  <a href="http://www.ncipher.com/support/advisories/advisory10.htm">http://www.ncipher.com/support/advisories/advisory10.htm</a></p> <p>There is no exploit code required.</p>	netHSM Logged Passphrase Information Disclosure
Low	3Com Corporation <sup>190</sup>  SuperStack 3 Switch, Switch 4400.0 SE, 4400.0 PWR, 4400.0 FX, 4400.0	<p>A remote Denial of Service vulnerability exists in the WEB management interface due to a failure to handle exceptional input.</p> <p>Updates available at:  <a href="http://csoweb4.3com.com/swups/">http://csoweb4.3com.com/swups/</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	3Com SuperStack Switch Remote Denial of Service
Low	D-Link <sup>191</sup>  DI-604, DI-614+ 2.30	<p>A remote Denial of Service vulnerability exists when a malicious user floods the device with specially crafted DHCP packets.</p> <p>No workaround or patch available at time of publishing.</p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	D-Link DI-614+ Router Denial of Service
Low	Enterasys <sup>192</sup>  XSR-1805 7.0 .0.0, 1850 7.0 .0.0	<p>A remote Denial of Service vulnerability exists due to a failure to handle IP packets with option 7 'Record Route.'</p> <p>No workaround or patch available at time of publishing.</p> <p>There is no exploit code required.</p>	Enterasys XSR-1800 Security Router Remote Denial of Service
Low	Juniper Networks <sup>193</sup>  JUNOS 6.1-6.3	<p>A remote Denial of Service vulnerability exists to a memory leak within the IPv6 Packet Forwarding Engine (PFE) when processing certain IPv6 packets.</p> <p>Juniper Networks has reported that all JUNOS software built on or after June 21, 2004 includes the corrected code. Customers are advised to contact the vendor to obtain fixes available at:  <a href="https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2004-06-009&amp;actionBtn=Search">https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2004-06-009&amp;actionBtn=Search</a></p> <p>Currently we are not aware of any exploits for this vulnerability.</p>	<p>Juniper JUNOS Packet Forwarding Engine (PFE) IPv6 Remote Denial of Service</p> <p>CVE Name: CAN-2004-0468</p>

<sup>189</sup> nCipher Security Advisory, No. 10, June 21, 2004.

<sup>190</sup> Secunia Advisory, SA11934, June 24, 2004.

<sup>191</sup> Bugtraq, June 28, 2004.

<sup>192</sup> Secunia Advisory, SA12014, July 6, 2004.

<sup>193</sup> VU#658859, <http://www.kb.cert.org/vuls/id/658859>.

Risk*	Vendor & Software Name	Multiple/Other Operating Systems Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name
Low	Multiple Vendors <sup>194</sup> Linksys Microsoft NetGeat  Linksys BEFSR41 v1-v3, Router 1.0 5.00, 1.35, 1.36, EtherFast BEFSR41 Router 1.37, 1.38, 1.39, 1.40.2, 1.41, 1.42.3, 1.42.7, 1.43, 1.43.3, 1.44, 1.45.7; Microsoft MN-500; NetGear FVS318 1.0, 1.1-1.3	A remote Denial of Service vulnerability exists in the web-based administration interface when multiple connections are submitted to port 80.  No workaround or patch available at time of publishing.  There is no exploit code required.	Multiple Vendor Broadband Router Web-Based Administration Denial of Service
Low	ZyXEL <sup>195</sup>  Prestige 650HW-31, 650R-11	A remote Denial of Service vulnerability exists in the authentication interface due to insufficient boundary checks on password string data.  No workaround or patch available at time of publishing.  There is no exploit code required.	ZyXEL Prestige Router Authentication Interface Remote Denial of Service

\*"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.

<sup>194</sup> Bugtraq, June 21, 2004.

<sup>195</sup> Secunia Advisory, SA11984, July 1, 2004.

## Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between June 21 and June 29, 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 12 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
<b>June 29, 2004</b>	<b>IMall.pl</b>	<b>Perl script that exploits the I-Mall Input Validation vulnerability.</b>
June 29, 2004	phpmy -explt.c	Script that exploits the phpMyAdmin Multiple Input Validation vulnerabilities.
<b>June 25, 2004.</b>	<b>JREFontObjectAssertionExploit.java</b>	<b>Proof of Concept script that exploits the Sun Java Runtime Environment Font Object Denial of Service vulnerability.</b>
June 25, 2004	Weplab-0.0.6-alpha.tar.gz	A tool to review the security of WEP encryption in wireless networks from an educational point of view. Several attacks are available to help measure the effectiveness and minimum requirements necessary to succeed.
June 24, 2004	rlprd.py	Exploit for the Rlpr Multiple Vulnerabilities.
<b>June 23, 2004</b>	<b>freebsd-alpha-dos.c</b>	<b>Script that exploits the FreeBSD execve() Denial of Service vulnerability.</b>
June 23, 2004	Hping3-alpha-2.tar.gz	A network tool designed to send custom ICMP/UDP/TCP packets and to display target replies like ping. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under all supported protocols. Using hping, you can test firewall rules, perform spoofed port scanning, etc.
June 23, 2004	Mod_rootme.0.2.tgz	A module that sets up a backdoor inside of Apache where a simple GET request will allow a remote administrator the ability to grab a root shell on the system without any logging.
June 23, 2004	Nmbscan-1.2.3.tar.gz	NMB Scanner scans the shares of a SMB network, using the NMB and SMB protocols.
June 23, 2004	Rkhunter-1.1.1.tar.gz	Rootkit Hunter scans files and systems for known and unknown rootkits, backdoors, and sniffers.
June 23, 2004	Unsecure.zip	Remote Proof of Concept Denial of Service exploit for the Epic Games Unreal Engine "Secure" Query Buffer Overflow vulnerability.
<b>June 21, 2004</b>	<b>code2.zip</b>	<b>Proof of Concept exploit for the Internet Explorer Non-FQDN URI Address Zone Bypass Vulnerability.</b>
June 21, 2004	monitUsernameBufferOverflowExpl.c	Script that exploits the TildeSlash Monit Authentication Buffer Overflow vulnerability.

## Trends

- US-CERT is aware of activity affecting compromised web sites running Microsoft's Internet Information Server (IIS) 5 and end-user systems that visit these sites. Compromised sites are appending JavaScript to the bottom of web pages. Web server administrators running IIS 5 should verify that there is no unusual JavaScript appended to the bottom of pages delivered by their web server. For more information, see TA04-184A located at: <http://www.us-cert.gov/cas/techalerts/TA04-184A.html>.
- US-CERT continues to receive reports of variants of a worm known as "W32/Korgo" or "W32/Padobot." This worm attempts to exploit a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). For more information see [http://www.us-cert.gov/current/current\\_activity.html](http://www.us-cert.gov/current/current_activity.html).
- US-CERT continues to receive reports of a worm known as "W32/Sasser." This worm attempts to exploit a buffer overflow vulnerability in the Windows Local Security Authority Service Server (LSASS). For more information see [http://www.us-cert.gov/current/current\\_activity.html](http://www.us-cert.gov/current/current_activity.html).
- Cabir is the first-ever computer virus that is capable of spreading over mobile phone networks. It is a network worm that infects phones running the Symbian mobile phone operating system by Symbian.
- **Fraudulent e-mails designed to dupe Internet users out of their credit card details or bank information topped the three billion mark last month, according to one of the largest spam e-mail filtering companies. The authentic-looking e-mails, masquerading as messages from banks or online retailers, have become a popular new tool for tech-savvy fraudsters in a new scam known as "phishing."**

## Viruses/Trojans

The following table encompasses new viruses, variations of previously encountered viruses, and Trojans that have been discovered in the last two weeks. They are listed alphabetically by their name. While these viruses and Trojans might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. Readers should also contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. Following this table are write-ups of new viruses and Trojans that are considered to be a high level threat. *NOTE: At times, viruses and 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.*

Name	Aliases	Type
Agent.E		Trojan
AntiQFX		Trojan
Backdoor.Berbew.F	Backdoor.Padodor.gen	Trojan
Backdoor.Berbew.G		Trojan
Backdoor.Botex		Trojan
Backdoor.Hacarmy.D	Backdoor.Hackarmy.q	Trojan
BackDoor-CCL	Backdoor.Banito.g BDS/Banito.D	Trojan

Name	Aliases	Type
Cabrotor	Backdoor.Cabrotor.10.a Cabronator	Trojan
DeDown		Trojan
Downloader-LM		Trojan
Downloader-LY		Trojan
IRC.Kelebek		Trojan
IRC-Xevol		Internet Relay Chat Trojan
JS/Scob-A	Trojan.JS.Scob.a JS_SCOB.A	Java Script Trojan
JS_JECT.A	TrojanDownloader.JS.Small.d Exploit/DialogArg	Java Script Trojan
Needy.J	Java/Needy.J	Trojan
Needy.K	Java/Needy.K	Trojan
Needy.L	Java/Needy.L	Trojan
Needy.M	Java/Needy.M	Trojan
Needy.N	Java/Needy.N	Trojan
Padodor.W	Backdoor.Padodor.w TrojanSpy.Win32.Qukart	Trojan
Poetry		Trojan
PWSteal.Refest		Trojan
Scob  <i>See IIS 5 Web Server Compromises below.</i>	Download.Ject Exploit-MhtRedir.gen Exploit-DialogArg.gen JS.Scob.Trojan JS.Small.d JS.Toofer JS/Exploit-DialogArg.b JS/Scob JS/Small-D	Java Script Trojan
Siboco		Trojan
Spofer		Trojan
StartPage-DU!htm		Trojan
StartPage-DU!text		Trojan
StartPage-EA		Trojan
TROJ_REFEST.A	TrojanSpy/Win32.Small.AA	Trojan
Trojan.Boxed.D	DDos.Win32.Boxed.Gen	Trojan
Trojan.Chost		Trojan
Trojan.Ecure		Trojan
Trojan.Ecure.B		Trojan
Trojan.Errhijack		Trojan
Trojan.Otinet		Trojan
Trojan.Spabot		Trojan
TrojanDownloader.Win32.Small	Small	Trojan
Turown		Trojan
W32.Ainesey.A@mm	VBS.Entice WORM_YESENIA.A	Win32 Worm
W32.Bugbear.K@mm		Win32 Worm
W32.Doep.A		Win32 Worm
W32.Gaobot.AUS		Win32 Worm
W32.Korgo!gen		Win32 Worm
W32.Mota.A	W32.Mota.A@mm	Win32 Worm
W32.Randex.ATS	Backdoor.IRCBot.gen Backdoor:Win32/IRCBot	Win32 Worm

Name	Aliases	Type
W32.Randex.ATX		Win32 Worm
W32/Agobot-KC	Backdoor.Agobot.gen W32/Gaobot.worm.gen.f W32.HLLW.Gaobot.gen	Win32 Worm
W32/Agobot-KE	Backdoor.Agobot.gen W32/Gaobot.worm.gen.j virus Win32/Agobot.NBZ Trojan W32.HLLW.Gaobot.gen WORM_AGOBOT.KW	Win32 Worm
W32/Agobot-KG	Gaobot Nortonbot Phatbot Polybot.	Win32 Worm
W32/Bagle-AD	W32/Bagle.ad@MM Win32/Bagle.BA@mm I-Worm.Bagle.aa Win32/Bagle.Variant.Worm W32.Beagle.Y@mm WORM_BAGLE.AD W32/Bagle.ad@mm W32.Beagle.Z@mm W32/Bagle.ae@MM	Win32 Worm
W32/Korgo-S	Worm.Win32.Padobot.gen WORM_KORGO.S W32.Korgo.M W32/Korgo.worm.s Worm/Padobot.O	Win32 Worm
W32/Lovgate-AD	I-Worm.Lovgate.ae W32/Lovgate.ad@MM WORM_LOVGATE.Y Win32/Lovgate.Y@mm W32.Lovgate.Y@mm PE_LOVGATE.AD Win32:Lovgate-AC I-Worm/Lovgate.X W32.Lovgate.X@mm I-Worm.LovGate.x W32/Lovgate.ac@MM	Win32 Worm
W32/Lovgate-AH	I-Worm.LovGate.ah W32.Lovgate.Z@mm I-Worm.LovGate.ah W32/Lovgate.af@MM	Win32 Worm
W32/Lovgate-F		Win32 Worm
W32/Mota.worm	I-Worm.MoTa.a Trojan.Mobotu Win32:MuTa	Win32 Worm
W32/NetskyP-Dam	WORM_NETSKY.DAM	Win32 Worm
W32/Rbot-AS		Win32 Worm
W32/Rbot-CA	Spybot	Win32 Worm
W32/Rbot-CC	Sdbot spybot	Win32 Worm
W32/Rbot-CG		Win32 Worm
W32/Rbot-CP		Win32 Worm
W32/Rbot-CR	Backdoor.Rbot.gen W32/Sdbot.worm.gen.o	Win32 Worm
W32/Sdbot-JF		Win32 Worm
W32/Sdbot-JG	IRCBot Randex.	Win32 Worm

Name	Aliases	Type
W32/Sdbot-JP	IRCBot Gaobot.	Win32 Worm
W32/Sdbot-JS	Multidropper-KS Backdoor.SdBot.os IRC/SdBot.AXJ TrojanProxy.Win32.Ranky.am Troj/Ranck-Fam Backdoor.Ranky.H	Win32 Worm
W32/Spybot-CW	Backdoor.Agobot.gen W32.HLLW.Gaobot.gen	Win32 Worm
W32/Yesenio.worm!vbs		Win32 Worm
Webber.P	Backdoor.Berbew Backdoor.Padodor.gen Bck/Dodo.B Berbew.F Webber.S	Trojan
WORM_AGOBOT.NL		Internet Worm
WORM_EVAMAN.A	Win32/Evaman.A@mm I-Worm.Evaman.A W32.Evaman@mm Win32.Evaman W32/Evaman@MM W32/Evaman-A I-Worm.Evaman.a	Win32 Worm
WORM_KORGO.T	Worm.Win32.Korgo.9343.B	Win32 Worm
WORM_KORGO.U	Worm/Padobot.O Win32/Korgo.R.worm W32.Korgo.O Worm.Win32.Padobot.l W32/Korgo.worm Win32.Korgo.W Worm/Padobot.U	Win32 Worm
WORM_KORGO.V	W32.Korgo.V	Win32 Worm
WORM_LOVGATE.AF	W32/Lovgate.af2@MM	Win32 Worm

**IIS 5 Web Server Compromises:** US-CERT is aware of new activity affecting compromised web sites running Microsoft's Internet Information Server (IIS) 5 and possibly end-user systems that visit these sites. Compromised sites are appending JavaScript to the bottom of web pages. When executed, this JavaScript attempts to access a file hosted on another server. This file may contain malicious code that can affect the end-user's system. US-CERT is investigating the origin of the IIS 5 compromises and the impact of the code that is downloaded to end-user systems. Web server administrators running IIS 5 should verify that there is no unusual JavaScript appended to the bottom of pages delivered by their web server. This activity is another example of why end users must exercise caution when JavaScript is enabled in their web browser. Disabling JavaScript will prevent this activity from affecting an end-user's system, but may also degrade the appearance and functionality of some web sites that rely upon JavaScript. US-CERT recommends that end-users disable JavaScript unless it is absolutely necessary. Users should be aware that any web site, even those that may be trusted by the user, may be affected by this activity and thus contain potentially malicious code.