

Vulnerability Summary for the Week of March 10, 2008

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered	CVSS Score	Source & Patch Info
		Published		
Adobe -- Form Client Adobe -- Form Designer	Multiple unspecified vulnerabilities in Adobe Form Designer 5.0 and Form Client 5.0 allow remote attackers to execute arbitrary code via unknown vectors related to input validation.	unknown 2008-03-11	9.3	CVE-2007-6253 OTHER-REF BID

Adobe -- ColdFusion Adobe -- ColdFusion MX	The administrator interface for Adobe ColdFusion 8 and ColdFusion MX7 does not log failed authentication attempts, which makes it easier for remote attackers to conduct brute force attacks without detection.	unknown 2008-03-11	7.5	CVE-2008-1203 OTHER-REF BID
Airspan -- WiMax_ProST	The administration panel on the Airspan WiMax ProST 4.1 antenna with 6.5.38.0 software does not verify authentication credentials, which allows remote attackers to (1) upload malformed firmware or (2) bind the antenna to a different WiMAX base station via unspecified requests to forms under process_adv/.	unknown 2008-03-10	10.0	CVE-2008-1262 BUGTRAQ OTHER-REF CERT-VN BID FRSIRT SECUNIA XF
Alice -- Gate2_Plus_Wi-Fi	cp06_wifi_m_nocifr.cgi in the admin panel on the Alice Gate 2 Plus Wi-Fi router does not verify authentication credentials, which allows remote attackers to disable Wi-Fi encryption via a certain request.	unknown 2008-03-10	7.1	CVE-2008-1269 BUGTRAQ OTHER-REF OTHER-REF

ASG -- ASG-Sentry	Multiple buffer overflows in ASG-Sentry Network Manager 7.0.0 and earlier allow remote attackers to execute arbitrary code or cause a denial of service (crash) via (1) a long request to FxIAList on TCP port 6162, or (2) an SNMP request with a long community string to FxAgent on UDP port 6161.	unknown 2008-03-13	10.0	CVE-2008-1320 BUGTRAQ MILWORM OTHER-REF BID FRSIRT SECUNIA XF
ASG -- ASG-Sentry	The File Check Utility (fcheck.exe) in ASG-Sentry Network Manager 7.0.0 and earlier allows remote attackers to cause a denial of service (CPU consumption) or overwrite arbitrary files via a query string that specifies the -b option, probably due to an argument injection vulnerability.	unknown 2008-03-13	7.8	CVE-2008-1322 BUGTRAQ MILWORM OTHER-REF BID FRSIRT SECUNIA XF
B21Soft -- BFup	Buffer overflow in the BFup ActiveX control (BFup.dll) in B21Soft BFup before 1.0.802.29 allows remote attackers to execute arbitrary code via a long FilePath parameter.	unknown 2008-03-10	9.3	CVE-2008-1282 OTHER-REF BID FRSIRT SECUNIA XF

	The control panel on the Belkin F5D7230-4 router with firmware 9.01.10 maintains authentication state by IP address, which allows remote attackers to bypass authentication by establishing a session from a source IP address of a previously authenticated user, a different vulnerability than CVE-2005-3802.	unknown 2008-03-10	10.0	CVE-2008-1242 BUGTRAQ OTHER-REF
Belkin -- F5D7230-4	cgi-bin/setup_dns.exe on the Belkin F5D7230-4 router with firmware 9.01.10 does not require authentication, which allows remote attackers to perform administrative actions, as demonstrated by changing a DNS server via the dns1_1, dns1_2, dns1_3, and dns1_4 parameters.	unknown 2008-03-10	10.0	CVE-2008-1244 BUGTRAQ OTHER-REF OTHER-REF
Belkin -- F5D7230-4	cgi-bin/setup_virtualserver.exe on the Belkin F5D7230-4 router with firmware 9.01.10 allows remote attackers to cause a denial of service (control center outage) via an HTTP request with invalid POST data and a	unknown 2008-03-10	7.8	CVE-2008-1245 BUGTRAQ OTHER-REF

	"Connection: Keep-Alive" header.			
Bloo -- Bloo	Multiple SQL injection vulnerabilities in index.php in Bloo 1.00 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) post_id, (2) post_category_id, (3) post_year_month, and (4) static_page_id parameters; and unspecified other vectors.	unknown 2008-03-12	7.5	CVE-2008-1313 MILWORM BID
BMscripts -- BM Classifieds	Multiple SQL injection vulnerabilities in BM Classifieds 20080309 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) cat parameter to showad.php and the (2) ad parameter to pfriendly.php.	unknown 2008-03-10	7.5	CVE-2008-1272 MILWORM SECUNIA
BT -- Home Hub	cgi/b on the BT Home Hub router allows remote attackers to bypass authentication, and read or modify administrative settings or make arbitrary VoIP telephone calls, by placing a character at the end of the PATH_INFO, as demonstrated by	unknown 2008-03-13	7.5	CVE-2008-1334 BUGTRAQ OTHER-REF OTHER-

	(1) %5C (encoded backslash), (2) '%' (percent), and (3) '~' (tilde). NOTE: the '/' (slash) vector is already covered by CVE-2007-5383.			REF
D-Link -- DI-524	Multiple buffer overflows in the web interface on the D-Link DI-524 router allow remote attackers to cause a denial of service (device crash) or possibly have unspecified other impact via (1) a long username or (2) an HTTP header with a large name and an empty value.	unknown 2008-03-10	7.8	CVE-2008-1266 BUGTRAQ OTHER-REF
Deutsche Telekom -- Speedport_W500_DSL_Router	b_banner.stm (aka the login page) on the Deutsche Telekom Speedport W500 DSL router allows remote attackers to obtain the logon password by reading the pwd field in the HTML source.	unknown 2008-03-10	10.0	CVE-2008-1252 BUGTRAQ OTHER-REF
Dokeos -- Open Source Learning and Knowledge Management Tool	Unspecified vulnerability in Dokeos 1.8.4 before SP3 allows attackers to execute arbitrary code via unspecified vectors.	unknown 2008-03-10	7.5	CVE-2008-1223 OTHER-REF OTHER-REF BID FRSIRT SECUNIA

eWriting -- eWriting Joomla -- com_ewriting Mambo -- com_ewriting	SQL injection vulnerability in index.php in the eWriting (com_ewriting) 1.2.1 module for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the cat parameter in a selectcat action.	unknown 2008-03-12	7.5	CVE-2008-1297 MILWORM BID SECUNIA
Gallarific -- Gallarific	Gallarific does not require authentication for (1) users.php and (2) index.php, which allows remote attackers to add and edit tasks via a direct request. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-13	7.5	CVE-2008-1327 OTHER-REF BID XF
IBM -- AIX	Untrusted search path vulnerability in man in IBM AIX 6.1.0 invokes binaries without full pathnames, which allows local users to execute arbitrary code via a malicious program in the man directory.	unknown 2008-03-10	7.2	CVE-2008-1274 AIXAPAR FRSIRT SECUNIA BID XF

JSPWiki -- JSPWiki	Unrestricted file upload vulnerability in JSPWiki 2.4.104 and 2.5.139 allows remote attackers to upload and execute arbitrary .jsp files via an unspecified manipulation that attaches a .jsp file to an "entry page."	unknown 2008-03-10	9.3	CVE-2008-1230 BUGTRAQ MILWORM OTHER-REF BID SECUNIA XF
JSPWiki -- JSPWiki	Directory traversal vulnerability in Edit.jsp in JSPWiki 2.4.104 and 2.5.139 allows remote attackers to include and execute arbitrary local .jsp files, and obtain sensitive information, via a .. (dot dot) in the editor parameter.	unknown 2008-03-10	9.3	CVE-2008-1231 BUGTRAQ MILWORM OTHER-REF BID SECUNIA XF
Kingssoft -- Antivirus Online Update Module	Heap-based buffer overflow in the KUpdateObj2 Class ActiveX control in UpdateOcx2.dll in Beijing KingSoft Antivirus Online Update Module 2007.12.29.29 allows remote attackers to execute arbitrary code via a long argument to the SetUninstallName method.	unknown 2008-03-12	7.5	CVE-2008-1307 MILWORM BID SECUNIA

Koobi -- Koobi CMS	SQL injection vulnerability in Koobi CMS 4.2.3 through 4.3.0 allows remote attackers to execute arbitrary SQL commands via the categ parameter in a links action to index.php, a different vector than CVE-2008-1122.	unknown 2008-03-13	7.5	CVE-2008-1336 MILWORM
Linksys -- WAG54GS	The Cisco Linksys WAG54GS Wireless-G ADSL Gateway with 1.01.03 and earlier firmware has "admin" as its default password for the "admin" account, which makes it easier for remote attackers to obtain access.	unknown 2008-03-13	7.5	CVE-2007-6709 BUGTRAQ OTHER-REF OTHER-REF
Linksys -- WRT54G	The web interface on the Linksys WRT54g router with firmware 1.00.9 does not require credentials when invoking scripts, which allows remote attackers to perform arbitrary administrative actions via a direct request to (1) Advanced.tri, (2) AdvRoute.tri, (3) Basic.tri, (4) ctlog.tri, (5) ddns.tri, (6) dmz.tri, (7) factdefa.tri, (8) filter.tri, (9) fw.tri, (10) manage.tri, (11) ping.tri, (12) PortRange.tri, (13) ptrigger.tri, (14) qos.tri, (15)	unknown 2008-03-10	10.0	CVE-2008-1247 BUGTRAQ OTHER-REF OTHER-REF

	rstatus.tri, (16) tracert.tri, (17) vpn.tri, (18) WanMac.tri, (19) WBasic.tri, or (20) WFilter.tri. NOTE: the Security.tri vector is already covered by CVE-2006-5202.			
Linksys -- WRT54G	The Linksys WRT54G router has "admin" as its default FTP password, which allows remote attackers to access sensitive files including nvram.cfg, a file that lists all HTML documents, and an ELF executable file.	unknown 2008-03-10	7.5	CVE-2008-1264 BUGTRAQ OTHER-REF
Linksys -- WRT54G	The Linksys WRT54G router allows remote attackers to cause a denial of service (device restart) via a long username and password to the FTP interface.	unknown 2008-03-10	7.8	CVE-2008-1265 BUGTRAQ OTHER-REF
Linksys -- WRT54G	The FTP server on the Linksys WRT54G 7 router with 7.00.1 firmware does not verify authentication credentials, which allows remote attackers to establish an FTP session by sending an arbitrary username and password.	unknown 2008-03-10	10.0	CVE-2008-1268 BUGTRAQ OTHER-REF OTHER-REF

<p>MailEnable -- MailEnable Enterprise MailEnable -- MailEnable Standard MailEnable -- MailEnable Professional</p>	<p>Multiple unspecified vulnerabilities in the SMTP service in MailEnable Standard Edition 1.x, Professional Edition 3.x and earlier, and Enterprise Edition 3.x and earlier allow remote attackers to cause a denial of service (crash) via crafted (1) EXPN or (2) VRFY commands.</p>	<p>unknown 2008-03-10</p>	<p>7.8</p>	<p>CVE-2008-1275 OTHER-REF BID FRSIRT SECUNIA</p>
<p>MailEnable -- MailEnable Enterprise MailEnable -- MailEnable Professional</p>	<p>Multiple buffer overflows in the IMAP service (MEIMAPS.EXE) in MailEnable Professional Edition and Enterprise Edition 3.13 and earlier allow remote authenticated attackers to execute arbitrary code via long arguments to the (1) FETCH, (2) EXAMINE, and (3) UNSUBSCRIBE commands.</p>	<p>unknown 2008-03-10</p>	<p>9.0</p>	<p>CVE-2008-1276 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA</p>
<p>MailEnable -- MailEnable Enterprise MailEnable -- MailEnable Professional</p>	<p>The IMAP service (MEIMAPS.exe) in MailEnable Professional Edition and Enterprise Edition 3.13 and earlier allows remote attackers to cause a denial of service (crash) via (1) SEARCH and (2) APPEND commands without required arguments, which triggers a NULL pointer dereference.</p>	<p>unknown 2008-03-10</p>	<p>9.0</p>	<p>CVE-2008-1277 BUGTRAQ OTHER-REF BID FRSIRT SECTRACK SECUNIA</p>

mapbender -- mapbender	Multiple SQL injection vulnerabilities in Mapbender 2.4 through 2.4.4 allow remote attackers to execute arbitrary SQL commands via the gaz parameter to mod_gazetteer_edit.php and other unspecified vectors.	unknown 2008-03-11	7.5	CVE-2008-0301 BUGTRAQ OTHER-REF
Matroska -- Demuxer	Buffer overflow in the Matroska demuxer (demuxers/demux_matroska.c) in xine-lib before 1.1.10 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code or via a Matroska file with invalid frame sizes.	unknown 2008-03-10	9.3	CVE-2008-1161 OTHER-REF
Microsoft -- Visual Studio .NET Microsoft -- Internet_Security_and_Acceleration_Server Microsoft -- Office Microsoft -- commerce_server Microsoft -- BizTalk Server	Unspecified vulnerability in certain COM objects in Microsoft Office Web Components 2000 allows user-assisted remote attackers to execute arbitrary code via vectors related to DataSource that trigger memory corruption, aka "Office Web Components DataSource Vulnerability."	unknown 2008-03-11	9.3	CVE-2007-1201 MS CERT BID FRSIRT SECUNIA

Microsoft -- Office	<p>Unspecified vulnerability in Microsoft Outlook in Office 2000 SP3, XP SP3, 2003 SP2 and Sp3, and Office System allows user-assisted remote attackers to execute arbitrary code via a crafted mailto URI.</p>	<p>unknown 2008-03-11</p>	9.3	CVE-2008-0110 MS CERT CERT-VN BID FRSIRT SECUNIA
<p>Microsoft -- Office Microsoft -- Excel Microsoft -- excel_viewer Microsoft -- Office_compatibility_pack_for_word_excel_ppt_2007</p>	<p>Unspecified vulnerability in Microsoft Excel 2000 SP3 through 2007, Viewer 2003, Compatibility Pack, and Office 2004 for Mac allows user-assisted remote attackers to execute arbitrary code via crafted data validation records, aka "Excel Data Validation Record Vulnerability."</p>	<p>unknown 2008-03-11</p>	9.3	CVE-2008-0111 MS CERT BID FRSIRT
<p>Microsoft -- Office Microsoft -- Excel</p>	<p>Unspecified vulnerability in Microsoft Excel 2000 SP3, and Office for Mac 2004 and 2008 allows user-assisted remote attackers to execute arbitrary code via a crafted .SLK file that is not properly handled when importing the file, aka "Excel File Import Vulnerability."</p>	<p>unknown 2008-03-11</p>	9.3	CVE-2008-0112 MS CERT BID FRSIRT

	Unspecified vulnerability in Microsoft Office Excel Viewer 2003 up to SP3 allows user-assisted remote attackers to execute arbitrary code via an Excel document with crafted cells that trigger memory corruption from an "allocation error," aka "Microsoft Office Cell Parsing Memory Corruption Vulnerability."	unknown 2008-03-11	9.3	CVE-2008-0113 MS CERT FRSIRT SECUNIA
Microsoft -- Office Microsoft -- Excel Microsoft -- excel_viewer	Unspecified vulnerability in Microsoft Excel 2000 SP3 through 2003 SP2, Viewer 2003, and Office for Mac 2004 allows user-assisted remote attackers to execute arbitrary code via crafted Style records that trigger memory corruption.	unknown 2008-03-11	9.3	CVE-2008-0114 MS CERT BID FRSIRT
Microsoft -- Office Microsoft -- Excel Microsoft -- excel_viewer Microsoft -- Office_compatibility_pack_for_word_excel_ppt_2007	Unspecified vulnerability in Microsoft Excel 2000 SP3 through 2007, Viewer 2003, Compatibility Pack, and Office for Mac 2004 allows user-assisted remote attackers to execute arbitrary code via malformed formulas, aka "Excel Formula Parsing Vulnerability."	unknown 2008-03-11	9.3	CVE-2008-0115 MS BID SECTRACK CERT FRSIRT

<p>Microsoft -- Office Microsoft -- Excel Microsoft -- excel_viewer Microsoft -- Office_compatibility_pack_for_word_excel_ppt_2007</p>	<p>Unspecified vulnerability in Microsoft Excel 2000 SP3 through 2003 SP2, Viewer 2003, Compatibility Pack, and Office 2004 and 2008 for Mac allows user-assisted remote attackers to execute arbitrary code via crafted rich text values, aka "Excel Rich Text Validation Vulnerability."</p>	<p>unknown 2008-03-11</p>	<p>9.3</p>	<p>CVE-2008-0116 MS CERT BID FRSIRT</p>
<p>Microsoft -- Office</p>	<p>Unspecified vulnerability in Microsoft Excel 2000 SP3 and 2002 SP2, and Office 2004 and 2008 for Mac, allows user-assisted remote attackers to execute arbitrary code via crafted conditional formatting values, aka "Excel Conditional Formatting Vulnerability."</p>	<p>unknown 2008-03-11</p>	<p>9.3</p>	<p>CVE-2008-0117 MS CERT BID FRSIRT</p>
<p>Microsoft -- Office</p>	<p>Unspecified vulnerability in Microsoft Office 2000 SP3, XP SP3, 2003 SP2, Excel Viewer 2003 up to SP3, and Office 2004 for Mac allows user-assisted remote attackers to execute arbitrary code via a crafted Office document that triggers memory corruption from an "allocation</p>	<p>unknown 2008-03-11</p>	<p>9.3</p>	<p>CVE-2008-0118 MS CERT BID FRSIRT SECUNIA</p>

	error," aka "Microsoft Office Memory Corruption Vulnerability."			
NetBSD -- NetBSD Current NetBSD -- NetBSD	The ipsec4_get_ulp function in the kernel in NetBSD 2.0 through 3.1 and NetBSD-current before 20071028, when the fast_ipsec subsystem is enabled, allows remote attackers to bypass the IPsec policy by sending packets from a source machine with a different endianness than the destination machine, a different vulnerability than CVE-2006-0905.	unknown 2008-03-13	9.3	CVE-2008-1335 NETBSD SECTRACK
PacketTrap -- PT360 Tool Suite	Directory traversal vulnerability in the TFTP server in PacketTrap Networks pt360 Tool Suite 1.1.33.1.0, and other versions before 2.0.3900.0, allows remote attackers to read and overwrite arbitrary files via directory traversal sequences in the pathname.	unknown 2008-03-12	10.0	CVE-2008-1310 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA XF

PHP-Nuke -- Hadith Module Kyantonius -- Hadith Module	SQL injection vulnerability in Hadith module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the cat parameter in a viewcat action to modules.php.	unknown 2008-03-12	7.5	CVE-2008-1298 BUGTRAQ OTHER-REF BID SECUNIA
PHP-Nuke -- NukeC Module	SQL injection vulnerability in the Sudirman Angriawan NukeC30 3.0 module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the id_catg parameter in a ViewCatg action to modules.php.	unknown 2008-03-12	7.5	CVE-2008-1308 BUGTRAQ BID
PHP-Nuke -- Gaestebuch Module	SQL injection vulnerability in the Johannes Hass gaestebuch 2.2 module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the id parameter in an edit action to modules.php.	unknown 2008-03-12	7.5	CVE-2008-1314 BUGTRAQ OTHER-REF BID
PHP-Nuke -- zClassifieds	SQL injection vulnerability in the ZClassifieds module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the cat parameter to modules.php.	unknown 2008-03-13	7.5	CVE-2008-1315 BUGTRAQ OTHER-REF BID

phpBB -- Filebase Module	SQL injection vulnerability in filebase.php in the Filebase mod for phpBB allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-03-12	7.5	CVE-2008-1305 MILWORM BID
QT-Cute -- QuickTalk Forum	SQL injection vulnerability in qtf_ind_search_ov.php in QT-cute QuickTalk Forum 1.6 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-03-13	7.5	CVE-2008-1316 MILWORM BID SECUNIA
RealNetworks -- RealPlayer	The RealAudioObjects. RealAudio ActiveX control in rmoc3260.dll 6.0.10.45 in RealNetworks RealPlayer 11.0.1 build 6.0.14.794 does not properly manage memory for the Console property, which allows remote attackers to execute arbitrary code or cause a denial of service (browser crash) via a series of assignments of long string values, which triggers an overwrite of freed heap memory. NOTE: some of these details are obtained from third party information.	unknown 2008-03-12	9.3	CVE-2008-1309 FULLDISC BID FRSIRT SECUNIA

SAP -- MaxDB	Integer signedness error in vserver in SAP MaxDB 7.6.0.37, and possibly other versions, allows remote attackers to execute arbitrary code via unknown vectors that trigger heap corruption.	unknown 2008-03-11	9.3	CVE-2008-0307 IDEFENSE BID SECTRACK FRSIRT SECUNIA
Siemens -- SpeedStream_6520	The Siemens SpeedStream 6520 router allows remote attackers to cause a denial of service (web interface crash) via an HTTP request to basehelp_English.htm with a large integer in the Content-Length field.	unknown 2008-03-10	7.8	CVE-2008-1267 BUGTRAQ OTHER-REF
SILC -- SILC Toolkit	Stack-based buffer overflow in the silc_fingerprint function in lib/silcutil/silcutil.c in Secure Internet Live Conferencing (SILC) Toolkit 1.1.5, and unspecified earlier versions, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via long input data. NOTE: some of these details are obtained from third party information.	unknown 2008-03-10	7.5	CVE-2008-1227 OTHER-REF OTHER-REF BID FRSIRT SECUNIA

Snom -- 320 SIP Phone	<p>snomControl.swf in the central phone server for the Snom 320 SIP Phone allows remote attackers to cause a denial of service (application crash and corruption of call logs) via a ""; (double quote, quote, close parenthesis, semicolon) sequence in the "Call a number" field.</p>	unknown 2008-03-10	9.4	CVE-2008-1249 BUGTRAQ OTHER-REF
Snom -- 320 SIP Phone	<p>Multiple cross-site request forgery (CSRF) vulnerabilities in the web interface on the central phone server for the Snom 320 SIP Phone allow remote attackers to perform actions as the phone user, as demonstrated by inserting an address-book entry containing an XSS sequence.</p>	unknown 2008-03-10	9.3	CVE-2008-1250 BUGTRAQ OTHER-REF
Sun -- Java Web Console	<p>Unspecified vulnerability in Sun Java Web Console 3.0.2, 3.0.3, and 3.0.4 allows remote attackers to bypass intended access restrictions and determine the existence of files or directories via unknown vectors.</p>	unknown 2008-03-11	7.8	CVE-2008-1286 SUNALERT BID FRSIRT SECUNIA XF

Travelsized -- Travelsized CMS	Multiple directory traversal vulnerabilities in index.php in Travelsized CMS 0.4.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) page_id and (2) language parameters.	unknown 2008-03-13	7.5	CVE-2008-1324 BUGTRAQ
Uberghey -- CMS	Multiple directory traversal vulnerabilities in index.php in Uberghey CMS 0.3.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) page_id and (2) language parameters.	unknown 2008-03-13	7.5	CVE-2008-1325 BUGTRAQ
Versant -- Versant Object Database	Untrusted search path and argument injection vulnerability in the VersantD service in Versant Object Database 7.0.1.3 and earlier, as used in Borland CaliberRM and probably other products, allows remote attackers to execute arbitrary commands via a request to TCP port 5019 with a modified VERSANT_ROOT field.	unknown 2008-03-13	9.3	CVE-2008-1319 BUGTRAQ BUGTRAQ MILWORM OTHER-REF BID FRSIRT SECUNIA XF

ZyXEL -- P-660HW	The ZyXEL P-660HW series router maintains authentication state by IP address, which allows remote attackers to bypass authentication by establishing a session from a source IP address of a previously authenticated user.	unknown 2008-03-10	10.0	CVE-2008-1255 BUGTRAQ OTHER-REF
ZyXEL -- P-660HW	The ZyXEL P-660HW series router has "admin" as its default password, which allows remote attackers to gain administrative access.	unknown 2008-03-10	10.0	CVE-2008-1256 BUGTRAQ OTHER-REF
ZyXEL -- P-2602HW-D1A	The Zyxel P-2602HW-D1A router with 3.40 (AJZ.1) firmware maintains authentication state by IP address, which allows remote attackers to bypass authentication by establishing a session from a source IP address of a user who previously authenticated within the previous 5 minutes.	unknown 2008-03-10	9.3	CVE-2008-1259 BUGTRAQ OTHER-REF

[Back to top](#)

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered	CVSS Score	Source & Patch Info
		Published		

Acronis -- True_Image	Acronis True Image Group Server 1.5.19.191 and earlier, included in Acronis True Image Enterprise Server 9.5.0.8072 and the other True Image packages, allows remote attackers to cause a denial of service (crash) via a packet with an invalid length field, which causes an out-of-bounds read.	unknown 2008-03-10	5.0	CVE-2008-1279 OTHER-REF FRSIRT SECUNIA BUGTRAQ XF
Acronis -- True_Image Acronis -- True_Image_Windows_Agent	Acronis True Image Windows Agent 1.0.0.54 and earlier, included in Acronis True Image Enterprise Server 9.5.0.8072 and the other True Image packages, allows remote attackers to cause a denial of service (crash) via a malformed packet to port 9876, which triggers a NULL pointer dereference.	unknown 2008-03-10	5.0	CVE-2008-1280 OTHER-REF FRSIRT SECUNIA BUGTRAQ XF
Adobe -- ColdFusion Adobe -- ColdFusion MX	Cross-site scripting (XSS) vulnerability in Adobe ColdFusion MX 7 and ColdFusion 8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-03-11	4.3	CVE-2008-0643 OTHER-REF BID
Adobe -- ColdFusion Adobe -- ColdFusion MX	Adobe ColdFusion MX 7 and ColdFusion 8 allows remote attackers to bypass the cross-site scripting (XSS) protection mechanism for applications via unspecified vectors related to the setEncoding function.	unknown 2008-03-11	5.0	CVE-2008-0644 OTHER-REF BID
Adobe -- LiveCycle Workflow	Cross-site scripting (XSS) vulnerability in the web management interface in Adobe LiveCycle Workflow 6.2 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	unknown 2008-03-11	4.3	CVE-2008-1202 BUGTRAQ OTHER-REF OTHER-REF
Alkacon -- OpenCms	Cross-site scripting (XSS) vulnerability in the Logfile Viewer Settings function in system/workplace/admin/workplace/logfileview/logfileViewSettings.jsp in Alkacon OpenCms 7.0.3 and 7.0.4 allows remote attackers to inject arbitrary web script or HTML via the filePath.0 parameter in a save action, a different vector than CVE-2008-1045.	unknown 2008-03-12	4.3	CVE-2008-1300 BUGTRAQ BID SECUNIA

Alkacon -- OpenCms	Absolute path traversal vulnerability in system/workplace/admin/workplace/logfileview/logfileViewSettings.jsp in Alkacon OpenCms 7.0.3 and 7.0.4 allows remote authenticated administrators to read arbitrary files via a full pathname in the filePath.0 parameter.	unknown 2008-03-12	5.0	CVE-2008-1301 BUGTRAQ BID SECUNIA
argontechnology -- Client_Management_Services	Directory traversal vulnerability in TFTPsrvs.exe 2.5.3.1 and earlier, as used in Argon Technology Client Management Services (CMS) 1.31 and earlier, allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter.	unknown 2008-03-10	5.0	CVE-2008-1281 OTHER-REF BID FRSIRT SECUNIA
ASG -- ASG-Sentry	The FxIAList service in ASG-Sentry Network Manager 7.0.0 and earlier does require authentication, which allows remote attackers to cause a denial of service (service termination) via the exit command to TCP port 6162, or have other impacts via other commands.	unknown 2008-03-13	5.0	CVE-2008-1321 BUGTRAQ MILWORM OTHER-REF BID FRSIRT SECUNIA XF
Besavvy -- Savvy Content Manager	Multiple cross-site scripting (XSS) vulnerabilities in Savvy Content Manager (CM) allow remote attackers to inject arbitrary web script or HTML via the searchterms parameter to (1) searchresults.cfm, (2) search_results.cfm, and (3) search_results/index.cfm. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-12	4.3	CVE-2008-1306 SECUNIA
BosDev -- BosClassifieds Classified Ads	Cross-site scripting (XSS) vulnerability in account.php in BosClassifieds Classified Ads System 3.0 allows remote attackers to inject arbitrary web script or HTML via the returnTo parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-10	4.3	CVE-2008-1224 SECUNIA

Cisco -- Finesse	The Cisco PIX/ASA Finesse Operation System 7.1 and 7.2 allows local users to gain privileges by entering characters at the enable prompt, erasing these characters via the Backspace key, and then holding down the Backspace key for one second after erasing the final character.	unknown 2008-03-10	6.8	CVE-2008-1246 BUGTRAQ OTHER-REF OTHER-REF
D-Link -- DSL-G604T	Cross-site scripting (XSS) vulnerability in cgi-bin/webcm on the D-Link DSL-G604T router allows remote attackers to inject arbitrary web script or HTML via the var: category parameter, as demonstrated by a request for advanced/portforw.htm on the fwan page.	unknown 2008-03-10	4.3	CVE-2008-1253 BUGTRAQ OTHER-REF
D-Link -- DI-604	Cross-site scripting (XSS) vulnerability in prim.htm on the D-Link DI-604 router allows remote attackers to inject arbitrary web script or HTML via the rf parameter.	unknown 2008-03-10	5.0	CVE-2008-1258 BUGTRAQ OTHER-REF
Dokeos -- Open Source Learning and Knowledge Management Tool	Cross-site scripting (XSS) vulnerability in Dokeos 1.8.4 before SP3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-03-10	4.3	CVE-2008-1222 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
Dovecot -- Dovecot	Argument injection vulnerability in Dovecot 1.0.x before 1.0.13, and 1.1.x before 1.1. rc3, when using blocking passdbs, allows remote attackers to bypass the password check via a password containing TAB characters, which are treated as argument delimiters that enable the skip_password_check field to be specified.	unknown 2008-03-10	6.8	CVE-2008-1218 MLIST MLIST
Encaps -- EncapsGallery	Multiple cross-site scripting (XSS) vulnerabilities in EncapsGallery 1.11.2 allow remote attackers to inject arbitrary web script or HTML via the file parameter to (1) watermark.php and (2) catalog_watermark.php in core/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-12	4.3	CVE-2008-1296 BID

Gallarific -- Gallarific	Cross-site scripting (XSS) vulnerability in search.php in Gallarific allows remote attackers to inject arbitrary web script or HTML via the query parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-13	4.3	CVE-2008-1326 OTHER-REF BID XF
Gregory Kokanosky -- phpMyNewsletter	SQL injection vulnerability in archives.php in Gregory Kokanosky (aka Greg's Place) phpMyNewsletter 0.8 beta 5 and earlier allows remote attackers to execute arbitrary SQL commands via the msg_id parameter.	unknown 2008-03-12	6.8	CVE-2008-1295 MILWORM BID
Horde -- Groupware Webmail Edition Horde -- Groupware Horde -- Horde	Directory traversal vulnerability in Horde 3.1.6, Groupware before 1.0.5, and Groupware Webmail Edition before 1.0.6, when running with certain configurations, allows remote authenticated users to read and execute arbitrary files via ".." sequences and a null byte in the theme name.	unknown 2008-03-10	6.0	CVE-2008-1284 BUGTRAQ BUGTRAQ MLIST MLIST MLIST BID FRSIRT SECUNIA XF
IBM -- Rational ClearQuest	IBM Rational ClearQuest 7.0.1.1 and 7.0.0.2 generates different error messages depending on whether the username is valid or invalid, which allows remote attackers to enumerate usernames.	unknown 2008-03-11	5.0	CVE-2008-1287 AIXAPAR BID FRSIRT SECUNIA XF
IBM -- Rational ClearQuest	IBM Rational ClearQuest 7.0.1.1 and 7.0.0.2 might allow local or remote attackers to obtain sensitive information about users by reading user cookies.	unknown 2008-03-11	5.0	CVE-2008-1288 AIXAPAR BID FRSIRT SECTRACK SECUNIA XF

ImageVue -- ImageVue	Multiple cross-site scripting (XSS) vulnerabilities in imageVue 1.7 allow remote attackers to inject arbitrary web script or HTML via the path parameter to (1) popup.php, (2) test/dir2.php, (3) admin/upload.php, and (4) dirxml.php in upload/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-10	4.3	CVE-2008-1273 OTHER-REF BID
JSPWiki -- JSPWiki	Cross-site scripting (XSS) vulnerability in Edit.jsp in JSPWiki 2.4.104 and 2.5.139 allows remote attackers to inject arbitrary web script or HTML via the editor parameter, a different vector than CVE-2007-5120.b.	unknown 2008-03-10	4.3	CVE-2008-1229 BUGTRAQ MILWORM OTHER-REF BID SECUNIA XF
lighttpd -- lighttpd	mod_userdir in lighttpd 1.4.18 and earlier, when userdir.path is not set, uses a default of \$HOME, which might allow remote attackers to read arbitrary files, as demonstrated by accessing the ~nobody directory.	unknown 2008-03-10	5.0	CVE-2008-1270 OTHER-REF OTHER-REF OTHER-REF
Linksys -- WAG54GS	Multiple cross-site scripting (XSS) vulnerabilities on the Cisco Linksys WAG54GS Wireless-G ADSL Gateway with 1.01.03 and earlier firmware allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2007-3574.	unknown 2008-03-13	4.3	CVE-2007-6707 BUGTRAQ OTHER-REF OTHER-REF
Linksys -- WAG54GS	Multiple cross-site request forgery (CSRF) vulnerabilities on the Cisco Linksys WAG54GS Wireless-G ADSL Gateway with 1.01.03 and earlier firmware allow remote attackers to perform actions as administrators via an arbitrary valid request to an administrative URI, as demonstrated by (1) a Restore Factory Defaults action using the mtenRestore parameter to setup.cgi and (2) creation of a user account using the sysname parameter to setup.cgi.	unknown 2008-03-13	4.3	CVE-2007-6708 BUGTRAQ OTHER-REF OTHER-REF

Linksys -- WRT300N	Cross-site scripting (XSS) vulnerability on the Linksys WRT300N router with firmware 2.00.20, when Mozilla Firefox or Apple Safari is used, allows remote attackers to inject arbitrary web script or HTML via the dyndns_domain parameter to the default URI.	unknown 2008-03-10	4.3	CVE-2008-1243 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF
ManageEngine -- ServiceDesk Plus	Cross-site scripting (XSS) vulnerability in SolutionSearch.do in ManageEngine ServiceDesk Plus 7.0.0 Build 7011 for Windows allows remote attackers to inject arbitrary web script or HTML via the searchText parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-03-12	4.3	CVE-2008-1299 BID SECUNIA
mapbender -- mapbender	mapFiler.php in Mapbender 2.4 to 2.4.4 allows remote attackers to execute arbitrary PHP code via PHP code sequences in the factor parameter, which are not properly handled when accessing a filename that contains those sequences.	unknown 2008-03-11	6.8	CVE-2008-0300 MILWORM OTHER-REF BID
MediaWiki -- MediaWiki	Unspecified vulnerability in MediaWiki 1.11 to 1.11.2 allows remote attackers to obtain sensitive "cross-site" information via the callback parameter in an API call for JavaScript Object Notation (JSON) formatted results.	unknown 2008-03-13	4.3	CVE-2008-1318 MLIST OTHER-REF BID FRSIRT SECTRACK SECUNIA XF
MiniGal -- MG2	Cross-site scripting (XSS) vulnerability in admin.php in MG2 (formerly Minigal) allows remote attackers to inject arbitrary web script or HTML via the list parameter in an import action.	unknown 2008-03-10	4.3	CVE-2008-1228 BUGTRAQ BID

PacketTrap -- PT360 Tool Suite Pro	The TFTP server in PacketTrap pt360 Tool Suite PRO 2.0.3901.0 and earlier allows remote attackers to cause a denial of service (daemon hang) by uploading a file named (1) ' ' (pipe), (2) "" (quotation mark), or (3) "<>" (less than, greater than); or (4) a file with a long name. NOTE: the issue for vector 4 might exist because of an incomplete fix for CVE-2008-1312.	unknown 2008-03-12	4.3	CVE-2008-1311 BUGTRAQ OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
PacketTrap -- PT360 Tool Suite	Unspecified vulnerability in the TFTP server in PacketTrap Networks pt360 Tool Suite 1.1.33.1.0, and other versions before 2.0.3900.0, allows remote attackers to cause a denial of service (daemon crash) via a long TFTP packet, a different vulnerability than CVE-2008-1311.	unknown 2008-03-12	5.0	CVE-2008-1312 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA
Perforce -- Perforce Server	The Perforce service (p4s.exe) in Perforce Server 2007.3/143793 and earlier allows remote attackers to cause a denial of service (daemon crash) via a (1) server-DiffFile or (2) server-ReleaseFile command with a large integer value, which is used in an array initialization calculation, and leads to invalid memory access.	unknown 2008-03-12	5.0	CVE-2008-1302 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA
Perforce -- Perforce Server	The Perforce service (p4s.exe) in Perforce Server 2007.3/143793 and earlier allows remote attackers to cause a denial of service (daemon crash) via a missing parameter to the (1) dm-FaultFile, (2) dm-LazyCheck, (3) dm-ResolvedFile, (4) dm-OpenFile, (5) crypto, and possibly unspecified other commands, which triggers a NULL pointer dereference.	unknown 2008-03-12	5.0	CVE-2008-1303 BUGTRAQ OTHER-REF OTHER-REF BID SECUNIA
redhat -- Directory Server	Red Hat Directory Server 7.1 before SP4 uses insecure permissions for certain directories, which allows local users to modify JAR files and execute arbitrary code via unknown vectors.	unknown 2008-03-11	4.6	CVE-2008-0890 REDHAT BID

RemotelyAnywhere -- RemotelyAnywhere	The RemotelyAnywhere.exe service in the Remotely Anywhere Server and Workstation 8.0.668 and earlier allows remote attackers to cause a denial of service (crash) via an invalid Accept-Charset header, which triggers a NULL pointer dereference. NOTE: the service is automatically restarted.	unknown 2008-03-10	5.0	CVE-2008-1278 OTHER-REF BID FRSIRT SECUNIA XF
SAP -- MaxDB	sdbstarter in SAP MaxDB 7.6.0.37, and possibly other versions, allows local users to execute arbitrary commands by using unspecified environment variables to modify configuration settings.	unknown 2008-03-11	6.9	CVE-2008-0306 IDEFENSE BID SECTRACK FRSIRT SECUNIA
silver-forge -- Neptune_Web_Server	Cross-site scripting (XSS) vulnerability in Neptune Web Server 3.0 allows remote attackers to inject arbitrary web script or HTML via the URI, which is not properly handled in the 404 error page.	unknown 2008-03-10	4.3	CVE-2008-1283 BUGTRAQ BID
Snom -- 320 SIP Phone	The web interface on the central phone server for the Snom 320 SIP Phone allows remote attackers to make arbitrary phone calls via the "Call a number" field. NOTE: this might overlap CVE-2007-3440.	unknown 2008-03-10	5.8	CVE-2008-1248 BUGTRAQ OTHER-REF
Snom -- 320 SIP Phone	Cross-site scripting (XSS) vulnerability in the web interface on the central phone server for the Snom 320 SIP Phone allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-03-10	4.3	CVE-2008-1251 BUGTRAQ OTHER-REF
Sun -- JSF	Cross-site scripting (XSS) vulnerability in Sun Java Server Faces (JSF) 1.2 before 1.2_08 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	unknown 2008-03-11	4.3	CVE-2008-1285 SUNALERT FRSIRT
Sun -- Solaris	Unspecified vulnerability in the Inter-Process Communication (IPC) message queue subsystem in Sun Solaris 10 allows local users to cause a denial of service (reboot) via blocked I/O message queues.	unknown 2008-03-13	4.9	CVE-2008-1317 SUNALERT BID FRSIRT SECUNIA

WebCT -- WebCT	Multiple cross-site scripting (XSS) vulnerabilities in WebCT Campus Edition 4.1.5.8, when "Don't wrap text" is enabled, allow remote authenticated users to inject arbitrary web script or HTML via a (1) mail message or (2) discussion board message. NOTE: this might overlap CVE-2005-1076.	unknown 2008-03-10	4.3	CVE-2008-1225 FULLDISC OTHER-REF OTHER-REF BID SECUNIA
WoltLab -- Burning Board Lite	Cross-site request forgery (CSRF) vulnerability in index.php in WoltLab Burning Board Lite (wBB) 2 Beta 1 allows remote attackers to delete threads as other users via the ThreadDelete action.	unknown 2008-03-13	4.3	CVE-2008-1323 BUGTRAQ XF
WordPress -- WordPress	Multiple cross-site scripting (XSS) vulnerabilities in WordPress 2.3.2 allow remote attackers to inject arbitrary web script or HTML via the (1) inviteemail parameter in an invite action to wp-admin/users.php and the (2) to parameter in a sent action to wp-admin/invites.php.	unknown 2008-03-12	4.3	CVE-2008-1304 BUGTRAQ OTHER-REF BID SECTRACK
Zimbra -- Collaboration_Suite	Multiple cross-site scripting (XSS) vulnerabilities in Zimbra Collaboration Suite (ZCS) 4.0.3, 4.5.6, and possibly other versions before 4.5.10 allow remote attackers to inject arbitrary web script or HTML via an e-mail attachment, possibly involving a (1) .jpg or (2) .gif image attachment.	unknown 2008-03-10	4.3	CVE-2008-1226 OTHER-REF OTHER-REF BID SECUNIA
ZyXEL -- P-660HW	Multiple cross-site request forgery (CSRF) vulnerabilities on the ZyXEL P-660HW series router allow remote attackers to (1) change DNS servers and (2) add keywords to the "bannedlist" via unspecified vectors.	unknown 2008-03-10	6.8	CVE-2008-1254 BUGTRAQ OTHER-REF
ZyXEL -- P-660HW	Cross-site scripting (XSS) vulnerability in Forms/DiagGeneral_2 on the ZyXEL P-660HW series router allows remote attackers to inject arbitrary web script or HTML via the PingIPAddr parameter.	unknown 2008-03-10	4.3	CVE-2008-1257 BUGTRAQ OTHER-REF

ZyXEL -- P-2602HW-D1A	Multiple cross-site request forgery (CSRF) vulnerabilities on the Zyxel P-2602HW-D1A router with 3.40(AJZ.1) firmware allow remote attackers to (1) make the admin web server available on the Internet (WAN) interface via the WWWAccessInterface parameter to Forms/RemMagWWW_1 or (2) change the IP whitelisting timeout via the StdioTimeout parameter to Forms/rpSysAdmin_1.	unknown 2008-03-10	6.8	CVE-2008-1260 BUGTRAQ OTHER-REF
ZyXEL -- P-2602HW-D1A	The Zyxel P-2602HW-D1A router with 3.40 (AJZ.1) firmware provides different responses to admin page requests depending on whether a user is logged in, which allows remote attackers to obtain current login status by requesting an arbitrary admin URI.	unknown 2008-03-10	5.0	CVE-2008-1261 BUGTRAQ OTHER-REF

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered	CVSS Score	Source & Patch Info
		Published		
Linksys -- WRT54G	The Linksys WRT54G router stores passwords and keys in cleartext in the Config.bin file, which might allow remote authenticated users to obtain sensitive information via an HTTP request for the top-level Config.bin URI.	unknown 2008-03-10	3.5	CVE-2008-1263 BUGTRAQ OTHER-REF

[Back to top](#)

Last updated March 17, 2008