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 Published	CVSS Score	Source & Patch Info
Apple -- Safari	Integer signedness error in Safari on Apple iPhone before 2.0 and iPod touch before 2.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving JavaScript array indices that trigger an out-of-bounds access, a different vulnerability than CVE-2008-2307.	unknown 2008-07-14	10.0	CVE-2008-2303 APPLE BID
Apple -- Safari	Unspecified vulnerability in WebCore in Safari on Apple iPhone before 2.0 and iPod touch before 2.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving style sheet elements that trigger memory corruption, probably during garbage collection, a different vulnerability than CVE-2008-1590.	unknown 2008-07-14	7.5	CVE-2008-2317 APPLE BID
auraCMS -- AuraCMS	js/pages/pages_data.php in AuraCMS 2.2 through 2.2.2 does not perform authentication, which allows remote attackers to add, edit, and delete web content via a modified id parameter.	unknown 2008-07-17	7.5	CVE-2008-3203 MILW0RM OTHER-REF BID XF
blackice -- black_ice_document_imaging_sdk	Heap-based buffer overflow in the OpenGifFile function in BiGif.dll in Black Ice Document Imaging SDK 10.95 allows remote attackers to execute arbitrary code via a long string argument to the GetNumberOfImagesInGifFile method in the BIImgFrm Control ActiveX control in biimgfrm.ocx. NOTE: some	unknown 2008-07-18	9.3	CVE-2008-3209 MILW0RM BID

	of these details are obtained from third party information.			
BoonEx -- ray	PHP remote file inclusion vulnerability in modules/global/inc/content.inc.php in BoonEx Ray 3.5, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the sIncPath parameter.	unknown 2008-07-14	9.3	CVE-2008-3166 MILW0RM FRSIRT
BoonEx -- Dolphin	Multiple PHP remote file inclusion vulnerabilities in BoonEx Dolphin 6.1.2, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) dir[plugins] parameter to (a) HTMLSax3.php and (b) safehtml.php in plugins/safehtml/ and the (2) sIncPath parameter to (c) ray/modules/global/inc/content.inc.php.	unknown 2008-07-14	9.3	CVE-2008-3167 MILW0RM BID
DreamLevels -- dreamnews_manager	SQL injection vulnerability in dreamnews-rss.php in DreamNews Manager allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-16	7.5	CVE-2008-3189 MILW0RM BID
e-topbiz -- million_pixels	SQL injection vulnerability in tops_top.php in E-topbiz Million Pixels 3 allows remote attackers to execute arbitrary SQL commands via the id_cat parameter.	unknown 2008-07-17	7.5	CVE-2008-3204 MILW0RM BID XF
easy-script -- avlc_forum	SQL injection vulnerability in vlc_forum.php in Avlc Forum as of 20080715 allows remote attackers to execute arbitrary SQL commands via the id parameter in an affich_message action.	unknown 2008-07-17	7.5	CVE-2008-3200 MILW0RM BID
Empire Server -- Empire Server	Multiple heap-based buffer overflows in Empire Server before 4.3.15 allow remote attackers to cause a denial of service or possibly execute arbitrary code via unspecified vectors, related to a "coordinate normalization bug." NOTE: some of these details are obtained from third party information.	unknown 2008-07-14	10.0	CVE-2008-3169 OTHER-REF OTHER-REF XF
F5 -- Firepass 1200	The SNMP daemon in the F5 FirePass 1200 6.0.2 hotfix 3 allows remote attackers to cause a denial of service (daemon crash) by walking the hrSWInstalled OID branch in HOST-RESOURCES-MIB.	unknown 2008-07-11	7.8	CVE-2008-3149 BUGTRAQ BID
FFmpeg -- FFmpeg	Stack-based buffer overflow in the str_read_packet function in libavformat/psxstr.c in FFmpeg before r13993 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a crafted STR file that interleaves audio and video sectors.	unknown 2008-07-14	9.3	CVE-2008-3162 OTHER-REF OTHER-REF

fuzzylime -- fuzzylime_cms	Directory traversal vulnerability in blog.php in fuzzylime (cms) 3.01, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the file parameter.	unknown 2008-07-14	7.6	CVE-2008-3164 OTHER-REF BID XF
gapi_cms -- gapicms	PHP remote file inclusion vulnerability in ktmlpro/includes/ktedit/toolbar.php in gapicms 9.0.2 allows remote attackers to execute arbitrary PHP code via a URL in the dirDepth parameter.	unknown 2008-07-15	7.5	CVE-2008-3183 BUGTRAQ MILW0RM FRSIRT
HP -- hpsi_active_directory_bidirectional_ldap_connector	Multiple unspecified vulnerabilities in HP Select Identity (HPSI) Active Directory Bidirectional LDAP Connector 2.20, 2.20.001, 2.20.002, and 2.30 allow remote attackers to execute arbitrary code via unspecified vectors.	unknown 2008-07-17	9.0	CVE-2008-1665
HP -- Oracle for OpenView	Unspecified vulnerability in HP Oracle for OpenView (OfO) 8.1.7, 9.1.01, 9.2, 9.2.0, 10g, and 10gR2 has unknown impact and attack vectors, possibly related to the July 2008 Oracle Critical Patch Update.	unknown 2008-07-17	10.0	CVE-2008-1666 HP
iamilkay -- yuhhu_pubs_black_cat	SQL injection vulnerability in browse.groups.php in Yuhhu Pubs Black Cat allows remote attackers to execute arbitrary SQL commands via the category parameter.	unknown 2008-07-18	7.5	CVE-2008-3206 BUGTRAQ BID XF
IBM -- data_ontap	Multiple unspecified vulnerabilities in IBM Data ONTAP 7.1 before 7.1.3, as used by IBM System Storage N series Filer and IBM System Storage N series Gateway, have unknown impact and attack vectors.	unknown 2008-07-14	10.0	CVE-2008-3160 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID XF XF
Mozilla -- Firefox	Mozilla Firefox 3.x before 3.0.1 allows remote attackers to inject arbitrary web script into a chrome document via unspecified vectors, as demonstrated by injection into a XUL error page. NOTE: this can be leveraged to execute arbitrary code using CVE-2008-2933.	unknown 2008-07-17	7.5	CVE-2008-3198 OTHER-REF OTHER-REF BID
neutrino-cms -- atomic_edition	Directory traversal vulnerability in index.php in Neutrino Atomic Edition 0.8.4 allows remote attackers to read and modify files, as demonstrated by manipulating data/sess.php in (1) usb and (2) del_pag actions. NOTE: this can be leveraged for code execution by performing an upload that bypasses the intended access restrictions that were implemented in sess.php.	unknown 2008-07-11	10.0	CVE-2008-3150 MILW0RM BID

Novell -- eDirectory	Heap-based buffer overflow in Novell eDirectory 8.7.3 before 8.7.3.10b, and 8.8 before 8.8.2 FTF2, allows remote attackers to execute arbitrary code via an LDAP search request containing "NULL search parameters."	unknown 2008-07-14	10.0	CVE-2008-1809 IDEFENSE BID
Novell -- eDirectory	Integer overflow in ds.dlm, as used by dhost.exe, in Novell eDirectory 8.7.3.10 before 8.7.3 SP10b and 8.8 before 8.8.2 ftf2 allows remote attackers to execute arbitrary code via unspecified vectors that trigger a stack-based buffer overflow, related to "flawed arithmetic."	unknown 2008-07-14	10.0	CVE-2008-3159 OTHER-REF OTHER-REF BID SECTRACK
Oracle -- weblogic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, and 9.0 has unknown impact and remote attack vectors.	unknown 2008-07-15	7.5	CVE-2008-2580 OTHER-REF
Oracle -- weblogic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 has unknown impact and remote attack vectors.	unknown 2008-07-15	7.5	CVE-2008-2582 OTHER-REF
Oracle -- Oracle Application Server Oracle -- oracle_portal_component	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3, 10.1.2.2, and 10.1.4.1 has unknown impact and remote attack vectors.	unknown 2008-07-15	7.5	CVE-2008-2589 OTHER-REF
Oracle -- Oracle Application Server Oracle -- oracle_portal_component	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 has unknown impact and remote attack vectors.	unknown 2008-07-15	7.5	CVE-2008-2594 OTHER-REF
Oracle -- times_ten_in_memory_database Oracle -- times_ten_client_server_component	Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2598 and CVE-2008-2599.	unknown 2008-07-15	10.0	CVE-2008-2597 OTHER-REF
Oracle -- times_ten_in_memory_database Oracle -- times_ten_client_server	Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2597 and CVE-2008-2599.	unknown 2008-07-15	7.5	CVE-2008-2598 OTHER-REF
Oracle -- times_ten_in_memory_database Oracle -- times_ten_client_server	Unspecified vulnerability in the TimesTen Client/Server component in Oracle Times Ten In-Memory Database 7.0.3.0.0 has unknown impact and remote attack vectors, a different vulnerability than CVE-2008-2597 and CVE-2008-2598.	unknown 2008-07-15	7.5	CVE-2008-2599 OTHER-REF

Oracle -- Oracle Application Server Oracle -- oracle_portal_component	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 9.0.4.3, 10.1.2.3, and 10.1.4.2 has unknown impact and remote attack vectors.	unknown 2008-07-15	7.5	CVE-2008-2609 OTHER-REF
Oracle -- Oracle Database Oracle -- core_rdbms_component	Unspecified vulnerability in the Core RDBMS component in Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.6 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	9.0	CVE-2008-2611 OTHER-REF
OrbitScripts -- SmartPPC Pro OrbitScripts -- SmartPPC	SQL injection vulnerability in directory.php in SmartPPC and SmartPPC Pro allows remote attackers to execute arbitrary SQL commands via the idDirectory parameter.	unknown 2008-07-11	7.5	CVE-2008-3152 MILW0RM BID XF
Panda -- Panda ActiveScan	Stack-based buffer overflow in the ActiveX control (as2guiie.dll) in Panda ActiveScan before 1.02.00 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a long argument to the Update method.	unknown 2008-07-11	9.3	CVE-2008-3155 FULLDISC FULLDISC MILW0RM OTHER-REF BID SECTRACK XF
Panda -- Panda ActiveScan	The ActiveScan ActiveX Control (as2guiie.dll) in Panda ActiveScan before 1.02.00 allows remote attackers to download and execute arbitrary cabinet (CAB) files via unspecified URLs passed to the Update method.	unknown 2008-07-11	9.3	CVE-2008-3156 FULLDISC FULLDISC MILW0RM OTHER-REF BID SECTRACK XF
resiprocate -- resiprocate	Multiple unspecified vulnerabilities in ReSIProcate before 1.3.4 allow remote attackers to cause a denial of service (stack consumption) via unknown network traffic with a large "bytes-in-memory/bytes-on-wire ratio."	unknown 2008-07-17	7.8	CVE-2008-3199 OTHER-REF
Sahil Ahuja -- pragyan_cms	PHP remote file inclusion vulnerability in cms/modules/form.lib.php in Pragyan CMS 2.6.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the (1) sourceFolder or (2) moduleFolder parameter.	unknown 2008-07-18	9.3	CVE-2008-3207 MILW0RM BID XF
sclek -- jsite	SQL injection vulnerability in jSite 1.0 OE allows remote attackers to execute arbitrary SQL commands via the page parameter to the default URI.	unknown 2008-07-16	7.5	CVE-2008-3193 MILW0RM BID XF
scripteen -- free_image_hosting_script	Scripteen Free Image Hosting Script 1.2 and 1.2.1 allows remote attackers to bypass authentication and gain administrative access by setting the cookid cookie value to 1.	unknown 2008-07-18	7.5	CVE-2008-3211 MILW0RM BID XF

scripteen -- free_image_hosting_script	Multiple SQL injection vulnerabilities in Scripteen Free Image Hosting Script 1.2.1 allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password parameter to admin/login.php, or the (3) uname or (4) pass parameter to login.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-18	7.5	CVE-2008-3212 BID XF
Sophos -- Sophos PureMessage Anti-Virus Sophos -- ES4000 Sophos -- Sophos Anti-Virus Sophos -- ES1000	Sophos virus detection engine 2.75 on Linux and Unix, as used in Sophos Email Appliance, Pure Message for Unix, and Sophos Anti-Virus Interface (SAVI), allows remote attackers to cause a denial of service (engine crash) via zero-length MIME attachments.	unknown 2008-07-15	7.8	CVE-2008-3177 OTHER-REF BID SECTRACK XF
SourceForge -- webxell_editor	Unrestricted file upload vulnerability in upload_pictures.php in WebXell Editor 0.1.3 allows remote attackers to execute arbitrary code by uploading a .php file with a jpeg content type, then accessing it via a direct request to the file in upload/.	unknown 2008-07-15	10.0	CVE-2008-3178 MILW0RM BID
speedbit -- download_accelerator_plus	Stack-based buffer overflow in DAP.exe in Download Accelerator Plus (DAP) 7.0.1.3, 8.6.6.3, and other 8.x versions allows user-assisted remote attackers to execute arbitrary code via an M3U (.m3u) file containing a long MP3 URL.	unknown 2008-07-15	9.3	CVE-2008-3182 MILW0RM MILW0RM BID XF
thekelleys -- dnsmasq	dnsmasq 2.25 allows remote attackers to cause a denial of service (1) renewing a non-existent lease or (2) sending a DHCPREQUEST for an IP address that is not in the same network.	unknown 2008-07-18	7.8	CVE-2008-3214 MLIST MLIST MLIST MLIST MLIST MLIST OTHER-REF OTHER-REF
tritoncms -- triton_cms_pro	SQL injection vulnerability in Triton CMS Pro allows remote attackers to execute arbitrary SQL commands via the X-Forwarded-For HTTP header.	unknown 2008-07-11	7.5	CVE-2008-3153 MILW0RM BID
W2B -- phpdatingclub	Directory traversal vulnerability in website.php in Web 2 Business (W2B) phpDatingClub (aka Dating Club) 3.7 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page argument.	unknown 2008-07-15	7.5	CVE-2008-3179 MILW0RM BID
WarpSpeed -- 4ndvddb PHPNuke -- 4ndvddb	SQL injection vulnerability in the 4ndvddb 0.91 module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the id parameter in a show_dvd action.	unknown 2008-07-11	7.5	CVE-2008-3151 BUGTRAQ BID

WebBlizzard -- Content Management System	SQL injection vulnerability in index.php in WebBlizzard CMS allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2008-07-11	7.5	CVE-2008-3154 MILW0RM BID XF
webcms -- webcms_portal_edition	SQL injection vulnerability in secciones/tablon/tablon.php in WebCMS Portal Edition allows remote attackers to execute arbitrary SQL commands via the id parameter to portal/index.php in a tablon action. NOTE: some of these details are obtained from third party information.	unknown 2008-07-18	7.5	CVE-2008-3213 MILW0RM BID
yacc -- yacc	skeleton.c in yacc does not properly handle reduction of a rule with an empty right hand side, which allows context-dependent attackers to cause an out-of-bounds stack access when the yacc stack pointer points to the end of the stack.	unknown 2008-07-16	7.8	CVE-2008-3196 MLIST MLIST

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
1scripts -- codedb	Directory traversal vulnerability in list.php in 1Scripts CodeDB 1.1.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	unknown 2008-07-16	6.8	CVE-2008-3190 MILW0RM BID XF
afuse -- afuse	The expand_template function in afuse.c in afuse 0.2 allows local users to gain privileges via shell metacharacters in a pathname.	unknown 2008-07-17	4.6	CVE-2008-2232 OTHER-REF
Apache Software Foundation -- Apache Microsoft -- IIS Sun -- Java System Web Server Sun -- ONE Web Server Oracle -- weblogic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server Plugins for Apache, Sun and IIS web servers component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, 7.0 SP7, and 6.1 SP7 has unknown impact and remote attack vectors.	unknown 2008-07-15	6.8	CVE-2008-2579 OTHER-REF
Apple -- Safari	Safari on Apple iPhone before 2.0 and iPod touch before 2.0 misinterprets a menu button press as user confirmation for visiting a web site with a (1) self-signed or (2) invalid certificate, which makes it easier for remote attackers to spoof web sites.	unknown 2008-07-14	4.3	CVE-2008-1589 APPLE BID
Apple -- core_image_fun_house	Buffer overflow in Apple Core Image Fun House 2.0 and earlier in CoreImage Examples in Xcode tools before 3.1 allows user-assisted attackers to execute arbitrary code or cause a denial of service (application crash) via a .funhouse file with a string XML element that contains	unknown 2008-07-14	6.8	CVE-2008-2304 BUGTRAQ MILW0RM OTHER-REF

	many characters.			
Apple -- Xcode Tools	The WOHyperlink implementation in WebObjects in Apple Xcode tools before 3.1 appends local session IDs to generated non-local URLs, which allows remote attackers to obtain potentially sensitive information by reading the requests for these URLs.	unknown 2008-07-14	5.0	CVE-2008-2318 OTHER-REF
Apple -- Safari	Apple Safari allows web sites to set cookies for country-specific top-level domains, such as co.uk and com.au, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session, aka "Cross-Site Cooking," a related issue to CVE-2004-0746, CVE-2004-0866, and CVE-2004-0867.	unknown 2008-07-14	6.8	CVE-2008-3170 OTHER-REF BID
Apple -- Safari	Apple Safari sends Referer headers containing https URLs to different https web sites, which allows remote attackers to obtain potentially sensitive information by reading Referer log data.	unknown 2008-07-14	4.3	CVE-2008-3171 OTHER-REF BID
Chipmunk Scripts -- Chipmunk Blogger	Multiple cross-site scripting (XSS) vulnerabilities in Chipmunk Blog (Blogger) allow remote attackers to inject arbitrary web script or HTML via the membername parameter to (1) members.php, (2) comments.php, (3) photos.php, (4) archive.php, or (5) cat.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-15	4.3	CVE-2008-3186 BID XF
content_now -- content_now	Unrestricted file upload vulnerability in upload.php in ContentNow CMS 1.4.1 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in upload/.	unknown 2008-07-15	6.5	CVE-2008-3181 MILW0RM BID
CWH Underground -- contentnow_cms	Multiple cross-site scripting (XSS) vulnerabilities in upload/file/language_menu.php in ContentNow CMS 1.4.1 allow remote attackers to inject arbitrary web script or HTML via the (1) pageid parameter or (2) PATH_INFO.	unknown 2008-07-15	4.3	CVE-2008-3180 MILW0RM BID
easy-script -- wysi_wiki_wyg	Directory traversal vulnerability in index.php in Easy-Script Wysi Wiki Wyg 1.0 allows remote attackers to read arbitrary files via a .. (dot dot) in the c parameter.	unknown 2008-07-17	5.0	CVE-2008-3205 MILW0RM BID XF
Empire Server -- Empire Server	The files utility in Empire Server before 4.3.15 discloses the world creation time, which makes it easier for attackers to determine the PRNG seed.	unknown 2008-07-14	5.0	CVE-2008-3168 XF

fuzzylime -- fuzzylime_cms	Directory traversal vulnerability in rss.php in fuzzylime (cms) 3.01a and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the p parameter, as demonstrated using content.php, a different vector than CVE-2007-4805.	unknown 2008-07-14	6.8	CVE-2008-3165 MILW0RM BID XF XF
IBM -- maximo	Multiple cross-site scripting (XSS) vulnerabilities in jsp/common/system/debug.jsp in IBM Maximo 4.1 and 5.2 allow remote attackers to inject arbitrary web script or HTML via the (1) Accept, (2) Accept-Language, (3) UA-CPU, (4) Accept-Encoding, (5) User-Agent, or (6) Cookie HTTP header. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-14	4.3	CVE-2008-3161 BID
marcioforum -- mforum	Multiple SQL injection vulnerabilities in usercp.php in mForum 0.1a, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) City, (2) Interest, (3) Email, (4) Icq, (5) msn, or (6) Yahoo Messenger field in an edit_profile action.	unknown 2008-07-16	6.8	CVE-2008-3191 MILW0RM BID XF
Microsoft -- ie	Microsoft Internet Explorer allows web sites to set cookies for domains that have a public suffix with more than one dot character, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session, aka "Cross-Site Cooking." NOTE: this issue may exist because of an insufficient fix for CVE-2004-0866.	unknown 2008-07-14	6.8	CVE-2008-3173 OTHER-REF OTHER-REF
Mozilla -- Firefox	Mozilla Firefox 3 before 3.0.1 on Mac OS X allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted GIF file that triggers a free of an uninitialized pointer.	unknown 2008-07-18	6.8	CVE-2008-2934 OTHER-REF OTHER-REF BID SECTRACK XF
Nortel -- sip_multimedia_pc_client	Nortel SIP Multimedia PC Client 4.x MCS5100 and MCS5200 does not limit the number of concurrent sessions, which allows attackers to cause a denial of service (resource consumption) via a large number of sessions.	unknown 2008-07-11	5.0	CVE-2008-3157 OTHER-REF OTHER-REF SECTRACK
Novell -- Novell Client for Windows	Unspecified vulnerability in NWFS.SYS in Novell Client for Windows 4.91 SP4 has unknown impact and attack vectors, possibly related to IOCTL requests that overwrite arbitrary memory.	unknown 2008-07-11	6.9	CVE-2008-3158 BID SECTRACK XF
OllyDbg -- OllyDbg mackt -- ImpRec	Stack-based buffer overflow in (1) OllyDBG 1.10 and (2) ImpREC 1.7f allows user-assisted attackers to execute arbitrary code via a crafted DLL file that	unknown 2008-07-11	6.8	CVE-2008-3148 MILW0RM BID

	contains a long string.			
opera -- opera	Opera allows web sites to set cookies for country-specific top-level domains that have DNS A records, such as co.tv, which could allow remote attackers to perform a session fixation attack and hijack a user's HTTP session, aka "Cross-Site Cooking."	unknown 2008-07-14	6.8	CVE-2008-3172 OTHER-REF OTHER-REF OTHER-REF OTHER-REF
Oracle -- weblogic_server Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 9.2, 9.1, 9.0, and 8.1 SP6 has unknown impact and local attack vectors.	unknown 2008-07-15	4.3	CVE-2008-2576 OTHER-REF
Oracle -- webloic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 9.2 MP1 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	4.6	CVE-2008-2577 OTHER-REF
Oracle -- webloic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 and 9.2 MP1 has unknown impact and local attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2578 OTHER-REF
Oracle -- weblogic_server_component Oracle -- bea_product_suite	Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 has unknown impact and remote attack vectors related to UDDI Explorer.	unknown 2008-07-15	5.1	CVE-2008-2581 OTHER-REF
Oracle -- application_server Oracle -- oracle_portal_component	Unspecified vulnerability in the sample Discussion Forum Portlet for the Oracle Portal component in Oracle Application Server, as available from OTN before 20080715, has unknown impact and remote attack vectors.	unknown 2008-07-15	4.3	CVE-2008-2583 OTHER-REF
Oracle -- E-Business Suite Oracle -- report_manager_component	Unspecified vulnerability in the Oracle Report Manager component in Oracle E-Business Suite 12.0.4 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2585 OTHER-REF
Oracle -- E-Business Suite Oracle -- application_object_library	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 12.0.4 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2586 OTHER-REF
Oracle -- Database 11g Oracle -- Database 9i Oracle -- Database 10g	Unspecified vulnerability in the Oracle Database Vault component in Oracle Database 9.2.0.8DV, 10.2.0.3, and 11.1.0.6 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2591
Oracle -- Oracle Database Oracle -- advanced_replication_component	Unspecified vulnerability in the Advanced Replication component in Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.6 has unknown impact and remote authenticated attack vectors related to SYS.DBMS_DEFER_SYS.	unknown 2008-07-15	6.5	CVE-2008-2592 OTHER-REF

Oracle -- Application Server 10g Oracle -- oracle_portal_component	Unspecified vulnerability in the Oracle Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 has unknown impact and remote attack vectors.	unknown 2008-07-15	4.3	CVE-2008-2593 OTHER-REF
Oracle -- Database 9i Oracle -- Database 10g	Unspecified vulnerability in the Oracle Internet Directory component in Oracle Application Server 9.0.4.3, 10.1.2.3, and 10.1.4.2 has unknown impact and remote attack vectors. NOTE: the previous information was obtained from the Oracle July 2008 CPU. Oracle has not commented on reliable researcher claims that this issue is a denial of service (crash) via a malformed LDAP request that triggers a NULL pointer dereference.	unknown 2008-07-15	5.0	CVE-2008-2595
Oracle -- E-Business Suite Oracle -- mobile_application_server	Unspecified vulnerability in the Mobile Application Server component in Oracle E-Business Suite 12.0.3 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2596 OTHER-REF
Oracle -- Oracle Database Oracle -- spatial_component	Unspecified vulnerability in the Oracle Spatial component in Oracle Database 10.1.0.5, 10.2.0.3, and 11.1.0.6 has unknown impact and remote authenticated attack vectors related to MDSYS.SDO_TOPO_MAP.	unknown 2008-07-15	6.5	CVE-2008-2600 OTHER-REF
Oracle -- E-Business Suite	Unspecified vulnerability in the Oracle iStore component in Oracle E-Business Suite 12.0.4 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	5.5	CVE-2008-2601
Oracle -- Database 11g Oracle -- data_pump_component Oracle -- Database 10g	Unspecified vulnerability in the Data Pump component in Oracle Database 10.1.0.5, 10.2.0.4, and 11.1.0.6 has unknown impact and remote authenticated attack vectors related to the IMP_FULL_DATABASE role.	unknown 2008-07-15	6.5	CVE-2008-2602 OTHER-REF
Oracle -- Database 11g Oracle -- authentication_component	Unspecified vulnerability in the Authentication component in Oracle Database 11.1.0.6 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2604 OTHER-REF
Oracle -- Database 11g Oracle -- authentication_component	Unspecified vulnerability in the Authentication component in Oracle Database 11.1.0.6 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2605 OTHER-REF
Oracle -- E-Business Suite Oracle -- application_object_library	Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 12.0.4 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2606 OTHER-REF
Oracle -- Database 11g Oracle -- advanced_queuing_component Oracle -- Database 9i Oracle -- Database 10g	Unspecified vulnerability in the Advanced Queuing component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.6 has unknown impact and remote authenticated attack vectors related to SYS.DBMS_AQELM. NOTE: the previous information was	unknown 2008-07-15	6.5	CVE-2008-2607 OTHER-REF

	obtained from the Oracle July 2008 CPU. Oracle has not commented on reliable researcher claims that this issue is a buffer overflow that allows attackers to cause a denial of service (database corruption) and possibly arbitrary code via a long argument to an unspecified procedure.			
Oracle -- data_pump_component Oracle -- Database 10g	Unspecified vulnerability in the Data Pump component in Oracle Database 10.1.0.5 and 10.2.0.3 has unknown impact and remote authenticated attack vectors related to SYS.KUPF$FILE_INT.	unknown 2008-07-15	6.5	CVE-2008-2608 OTHER-REF
Oracle -- E-Business Suite Oracle -- oracle_applications_technology_stack_component	Unspecified vulnerability in the Oracle Applications Technology Stack component in Oracle E-Business Suite 12.0.4 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2610 OTHER-REF
Oracle -- hyperion_bi_plus_component Oracle -- Oracle Application Server	Unspecified vulnerability in the Hyperion BI Plus component in Oracle Application Server 8.3.2.4, 8.5.0.3, 9.2.0.3, 9.2.1.0, and 9.3.1.0 has unknown impact and remote attack vectors.	unknown 2008-07-15	4.3	CVE-2008-2612 OTHER-REF
Oracle -- Database 11g Oracle -- database_scheduler Oracle -- Database 10g	Unspecified vulnerability in the Database Scheduler component in Oracle Database 10.2.0.4 and 11.1.0.6 has unknown impact and local attack vectors. NOTE: the previous information was obtained from the Oracle July 2008 CPU. Oracle has not commented on reliable researcher claims that this is an untrusted search path issue that allows local users to execute arbitrary code via a malicious library.	unknown 2008-07-15	6.5	CVE-2008-2613 OTHER-REF
Oracle -- oracle_http_server_component Oracle -- Oracle Application Server	Unspecified vulnerability in the Oracle HTTP Server component in Oracle Application Server 9.0.4.3, 10.1.2.3, and 10.1.3.3 has unknown impact and remote attack vectors.	unknown 2008-07-15	4.3	CVE-2008-2614 OTHER-REF
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2615 OTHER-REF
Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise Oracle -- PeopleSoft PeopleTools	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2616 OTHER-REF
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote	unknown 2008-07-15	6.5	CVE-2008-2617 OTHER-REF

	authenticated attack vectors.			
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2618 OTHER-REF
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2620 OTHER-REF
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	4.0	CVE-2008-2621 OTHER-REF
Oracle -- peoplesoft_peopletools_component Oracle -- JD Edwards EnterpriseOne Oracle -- PeopleSoft Enterprise	Unspecified vulnerability in the PeopleSoft PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.48.17 and 8.49.11 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	6.5	CVE-2008-2622 OTHER-REF
pagefusion -- pagefusion	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Pagefusion 1.5 allow remote attackers to inject arbitrary web script or HTML via the (1) acct_fname and (2) acct_lname parameters in an edit action, and the (3) PID, (4) PGID, and (5) rez parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-17	4.3	CVE-2008-3201 OTHER-REF BID XF
Pluck -- Pluck	Multiple directory traversal vulnerabilities in data/inc/themes/predefined_variables.php in pluck 4.5.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) langpref, (2) file, (3) blogpost, or (4) cat parameter.	unknown 2008-07-16	6.8	CVE-2008-3194 MILW0RM BID XF
regretless -- dodos_mail	Directory traversal vulnerability in dodosmail.php in DodosMail 2.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the dodosmail_header_file parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-14	6.8	CVE-2008-3163 BID XF
resiprocate -- resiprocate	rutil/dns/DnsStub.cxx in ReSIProcate 1.3.2, as used by repro, allows remote attackers to cause a denial of service (daemon crash) via a SIP (1) INVITE or (2) OPTIONS message with a long	unknown 2008-07-18	4.3	CVE-2008-3210 MILW0RM OTHER-REF BID XF

	domain name in a request URI, which triggers an assert error.			
sclek -- jsite	Directory traversal vulnerability in index.php in jSite 1.0 OE allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the module parameter.	unknown 2008-07-16	6.8	CVE-2008-3192 MILW0RM BID XF
simpledns -- simple_dns_plus	Simple DNS Plus 4.1, 5.0, and possibly other versions before 5.1.101 allows remote attackers to cause a denial of service via multiple DNS reply packets.	unknown 2008-07-18	5.0	CVE-2008-3208 BUGTRAQ MILW0RM OTHER-REF OTHER-REF BID XF
vbulletin -- vbulletin	Multiple cross-site scripting (XSS) vulnerabilities in vBulletin 3.6.10 PL2 and earlier, and 3.7.2 and earlier 3.7.x versions, allow remote attackers to inject arbitrary web script or HTML via (1) the PATH_INFO (PHP_SELF) or (2) the do parameter, as demonstrated by requests to upload/admincp/faq.php. NOTE: this issue can be leveraged to execute arbitrary PHP code.	unknown 2008-07-15	4.3	CVE-2008-3184 BUGTRAQ OTHER-REF BID
vclcomponents -- relative_real_estate_systems	SQL injection vulnerability in index.php in Relative Real Estate Systems 3.0 and earlier allows remote attackers to execute arbitrary SQL commands via the listing_id parameter in a listings action.	unknown 2008-07-15	6.8	CVE-2008-3185 MILW0RM OTHER-REF BID FRSIRT XF
WebKit -- javascriptcore	JavaScriptCore in WebKit on Apple iPhone before 2.0 and iPod touch before 2.0 does not properly perform runtime garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors that trigger memory corruption, a different vulnerability than CVE-2008-2317.	unknown 2008-07-14	6.8	CVE-2008-1590 APPLE BID
wefi -- wefi	WeFi 3.2.1.4.1, when diagnostic mode is enabled, stores (1) WEP, (2) WPA, and (3) WPA2 access-point keys in (a) ClientWeFiLog.dat, (b) ClientWeFiLog.bak, and possibly (c) a certain .inf file under %PROGRAMFILES%\WeFi\Users\, and uses cleartext for the ClientWeFiLog files, which allows local users to obtain sensitive information by reading these files.	unknown 2008-07-11	4.7	CVE-2008-3147 BUGTRAQ BUGTRAQ BID XF
xomol -- xomol_cms	Cross-site scripting (XSS) vulnerability in index.php in Xomol CMS 1.2 allows remote attackers to inject arbitrary web script or HTML via the current_url parameter in a tellafriend action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-17	4.3	CVE-2008-3202 OTHER-REF BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Mozilla -- Firefox	Mozilla Firefox before 2.0.0.16, and 3.x before 3.0.1, interprets '|' (pipe) characters in a command-line URI as requests to open multiple tabs, which allows remote attackers to access chrome:i URIs, or read arbitrary local files via manipulations involving a series of URIs that is not entirely handled by a vector application, as exploited in conjunction with CVE-2008-2540. NOTE: this issue exists because of an insufficient fix for CVE-2005-2267.	unknown 2008-07-17	2.6	CVE-2008-2933 OTHER-REF OTHER-REF BID
Oracle -- Database 9i Oracle -- advanced_replication Oracle -- Database 10g	Unspecified vulnerability in the Advanced Replication component in Oracle Database 9.0.1.5 FIPS+, 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 has unknown impact and local attack vectors.	unknown 2008-07-15	2.1	CVE-2008-2587 OTHER-REF
Oracle -- instance_management_component Oracle -- Enterprise Manager 10g Oracle -- Database 10g	Unspecified vulnerability in the Instance Management component in Oracle Database 10.1.0.5 and Enterprise Manager 10.1.0.6 has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	3.5	CVE-2008-2590 OTHER-REF
Oracle -- Enterprise Manager	Unspecified vulnerability in the Resource Manager component in Oracle Database 10.1.0.5, 10.2.0.4, and 11.1.0.6, and Database Control in Enterprise Manager, has unknown impact and remote authenticated attack vectors.	unknown 2008-07-15	3.5	CVE-2008-2603
phpMyAdmin -- phpMyAdmin	Cross-site request forgery (CSRF) vulnerability in phpMyAdmin before 2.11.7.1 allows remote attackers to perform unauthorized actions via a link or IMG tag to (1) the "Creating a Database" functionality (db_create.php) and (2) unspecified vectors that modify the connection character set.	unknown 2008-07-16	3.5	CVE-2008-3197 OTHER-REF OTHER-REF
Wireshark -- Wireshark	The fragment_add_work function in epan/reassemble.c in Wireshark 0.8.19 through 1.0.1 allows remote attackers to cause a denial of service (crash) via a series of fragmented packets with non-sequential fragmentation offset values, which lead to a buffer over-read.	unknown 2008-07-16	2.9	CVE-2008-3145 OTHER-REF OTHER-REF OTHER-REF OTHER-REF FEDORA BID SECTRACK XF

Back to top