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 (CVSS Score: 7.0 .. 10.0) | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| | Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka "Uninitialized Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0553 CERT |
| abk-soft -- ablespace | Multiple SQL injection vulnerabilities in AbleSpace 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) eid parameter to events_view.php and the (2) id parameter to events_clndr_view.php. | 2009-04-17 | 7.5 | CVE-2009-1316 BID BUGTRAQ MILW0RM MISC |
| ajsquare -- aj_article | SQL injection vulnerability in index.php in AJ Square AJ Article allows remote attackers to execute arbitrary SQL commands via the txtName parameter (aka the username field). | 2009-04-14 | 7.5 | CVE-2008-6721 XF BID MILW0RM |
| apache -- geronimo | Multiple directory traversal vulnerabilities in the web administration console in Apache Geronimo Application Server 2.1 through 2.1.3 on Windows allow remote attackers to upload files to arbitrary directories via directory traversal sequences in the (1) group, (2) artifact, (3) version, or (4) fileType parameter to | 2009-04- | 9.4 | CVE-2008-5518 |

| | | | | |
|---|---|---|---|---|
| apache -- geronimo | console/portal//Services/Repository (aka the Services/Repository portlet); the (5) createDB parameter to console/portal/Embedded DB/DB Manager (aka the Embedded DB/DB Manager portlet); or the (6) filename parameter to the createKeystore script in the Security/Keystores portlet. | 17 | 9.4 | CONFIRM<br>CONFIRM |
| argyllcms -- argyllcms<br>ghostscript -- ghostscript | Multiple integer overflows in icc.c in the International Color Consortium (ICC) Format library (aka icclib), as used in Ghostscript 8.64 and earlier and Argyll Color Management System (CMS) 1.0.3 and earlier, allow context-dependent attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly execute arbitrary code by using a device file for a translation request that operates on a crafted image file and targets a certain "native color space," related to an ICC profile in a (1) PostScript or (2) PDF file with embedded images. NOTE: this issue exists because of an incomplete fix for CVE-2009-0583. | 2009-04-14 | 9.3 | CVE-2009-0792<br>FEDORA<br>FEDORA<br>CONFIRM<br>REDHAT<br>SECUNIA<br>SECUNIA<br>SECUNIA |
| avaya -- communication_manager<br>avaya -- sip_enablement_services | Multiple unspecified vulnerabilities in the Web management interface in Avaya SIP Enablement Services (SES) 3.x and 4.0, as used with Avaya Communication Manager 3.1.x, allow remote attackers to obtain (1) application server configuration, (2) database server configuration including encrypted passwords, (3) a system utility that decrypts "subscriber table passwords," (4) a system utility that decrypts database passwords, and (5) a system utility that encrypts "subscriber table passwords." | 2009-04-10 | 7.8 | CVE-2008-6706<br>XF<br>XF<br>XF<br>XF<br>MISC<br>MISC<br>MISC<br>MISC<br>MISC<br>CONFIRM |
| china-on-site -- flexphplink | Unrestricted file upload vulnerability in submitlink.php in FlexPHPLink Pro 0.0.7 allows remote attackers to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a direct request to the renamed file in linkphoto/. | 2009-04-20 | 9.3 | CVE-2008-6731<br>XF<br>BID<br>OSVDB<br>MILW0RM<br>SECUNIA |
| cpcommerce -- cpcommerce | SQL injection vulnerability in document.php in cpCommerce 1.2.8 allows remote attackers to execute arbitrary SQL commands via the id_document parameter. | 2009-04-20 | 7.5 | CVE-2009-1345<br>XF<br>BID<br>MILW0RM |
| | Multiple stack-based buffer overflows in the Danske Bank e- | | | CVE-2008 |

| | | | | |
|---|---|---|---|---|
| danskebank -- danskesikker.ocx | Sec Control Module ActiveX control (DanskeSikker.ocx) 3.1.0.48, and possibly earlier versions, allow remote attackers to execute arbitrary code via long arguments to unspecified methods, which are not properly handled by a logging function. | 2009-04-16 | 9.3 | CVE-2008-1107<br>VUPEN<br>BID<br>BUGTRAQ<br>MISC<br>SECUNIA |
| debian -- apt | apt 0.7.20 does not check when the date command returns an "invalid date" error, which can prevent apt from loading security updates in time zones for which DST occurs at midnight. | 2009-04-16 | 10.0 | CVE-2009-1300<br>CONFIRM<br>MLIST<br>CONFIRM |
| deltascripts -- php_links | SQL injection vulnerability in admin/adm_login.php in DeltaScripts PHP Links 1.3 and earlier allows remote attackers to execute arbitrary SQL commands via the admin_username parameter (aka the admin field). | 2009-04-13 | 7.5 | CVE-2008-6720<br>BID<br>MILW0RM |
| divx -- divx_web_player | Integer signedness error in DivX Web Player 1.4.2.7, and possibly earlier versions, allows remote attackers to execute arbitrary code via a DivX file containing a crafted Stream Format (STRF) chunk, which triggers a heap-based buffer overflow. | 2009-04-16 | 9.3 | CVE-2008-5259<br>VUPEN<br>BID<br>BUGTRAQ<br>MISC<br>SECUNIA |
| emc -- replistor | Multiple heap-based buffer overflows in EMC RepliStor 6.2 before SP5 and 6.3 before SP2 allow remote attackers to execute arbitrary code via a crafted message to (1) ctrlservice.exe or (2) rep_srv.exe, possibly related to an integer overflow. | 2009-04-15 | 10.0 | CVE-2009-1119<br>VUPEN<br>SECTRACK<br>BID<br>BUGTRAQ<br>MISC<br>SECUNIA |
| filestream -- turbozip<br>hp -- openview_performance_agent<br>innermedia -- dynazip_max<br>innermedia -- dynazip_max_secure | Multiple stack-based buffer overflows in DZIP32.DLL before 5.0.0.8 in DynaZip Max and DZIPS32.DLL before 6.0.0.5 in DynaZip Max Secure; as used in HP OpenView Performance Agent C.04.60, HP Performance Agent C.04.70 and C.04.72, TurboZIP 6.0, and other products; allow user-assisted attackers to execute arbitrary code via a long filename in a ZIP archive during a (1) Fix (aka Repair), (2) Add, (3) Update, or (4) Freshen action, a related issue to CVE-2006-3985. | 2009-04-13 | 9.3 | CVE-2008-4420<br>BID<br>HP |
| freetype -- freetype | Multiple integer overflows in FreeType 2.3.9 and earlier allow remote attackers to execute arbitrary code via vectors related to large values in certain inputs in (1) smooth/ftsmooth.c, (2) sfnt/ttcmap.c, and (3) cff/cffload.c. | 2009-04-16 | 10.0 | CVE-2009-0946<br>CONFIRM |
| | Heap-based buffer overflow in the big2_decode_symbol_dict function (jbig2_symbol_dict.c) in the JBIG2 decoding library (jbig2dec) in | | | CVE-2009 |

| | | | | |
|---|---|---|---|---|
| ghostscript -- ghostscript | Ghostscript 8.64, and probably earlier versions, allows remote attackers to execute arbitrary code via a PDF file with a JBIG2 symbol dictionary segment with a large run length value. | 2009-04-16 | 9.3 | CVE-2009-0196 BID |
| guestcal -- guest_cal | Directory traversal vulnerability in includes/ini.inc.php in GuestCal 2.1 allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the lang parameter to index.php. | 2009-04-17 | 7.5 | CVE-2009-1319 BID MILW0RM SECUNIA |
| interguias -- nethoteles | SQL injection vulnerability in publico/ficha.php in NetHoteles 3.0 allows remote attackers to execute arbitrary SQL commands via the id_establecimiento parameter. | 2009-04-20 | 7.5 | CVE-2009-1346 XF BID MILW0RM |
| kernel -- udev | udev before 1.4.1 does not verify whether a NETLINK message originates from kernel space, which allows local users to gain privileges by sending a NETLINK message from user space. | 2009-04-17 | 7.2 | CVE-2009-1185 BID DEBIAN |
| microsoft -- windows_server_2003<br>microsoft -- windows_server_2008<br>microsoft -- windows_vista<br>microsoft -- windows_xp | The Windows Management Instrumentation (WMI) provider in Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka "Windows WMI Service Isolation Vulnerability." | 2009-04-15 | 7.2 | CVE-2009-0078 CERT |
| microsoft -- directx | DirectShow in Microsoft DirectX 8.1 and 9.0 does not properly decompress media files, which allows remote attackers to execute arbitrary code via a crafted MJPEG (1) file or (2) video stream, aka "MJPEG Decompression Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0084 CERT |
| microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_server_2008<br>microsoft -- windows_vista<br>microsoft -- windows_xp | Integer underflow in Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote HTTP servers to execute arbitrary code via crafted parameter values in a response, related to error handling, aka "Windows HTTP Services Integer Underflow Vulnerability." | 2009-04-15 | 10.0 | CVE-2009-0086 CERT |
| microsoft -- office_word | Unspecified vulnerability in the Word 6 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2; and the Word 6 text | | | |

| | | | | |
|---|---|---|---|---|
| microsoft -- windows<br>microsoft -- windows_server<br>microsoft -- windows_srv<br>microsoft -- windows_xp | converter in Microsoft Office Word 2000 SP3 and 2002 SP3; allows remote attackers to execute arbitrary code via a crafted Word 6 file that contains malformed data, aka "WordPad and Office Text Converter Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0087<br>CERT |
| microsoft -- office_converter_pack<br>microsoft -- office_word<br>microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_xp | The WordPerfect 6.x Converter in Microsoft Office Word 2000 SP3 and Microsoft Office Converter Pack does not properly validate the length of an unspecified string, which allows remote attackers to execute arbitrary code via a crafted WordPerfect 6.x file, aka "Word 2000 WordPerfect 6.x Converter Stack Corruption Vulnerability." | 2009-04-15 | 10.0 | CVE-2009-0088<br>CERT |
| microsoft -- office<br>microsoft -- office_compatibility_pack_for_word_excel_ppt_2007<br>microsoft -- office_excel<br>microsoft -- office_excel_viewer | Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1; Excel in Microsoft Office 2004 and 2008 for Mac; Microsoft Office Excel Viewer and Excel Viewer 2003 SP3; and Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1 do not properly parse the Excel spreadsheet file format, which allows remote attackers to execute arbitrary code via a crafted spreadsheet that contains a malformed object, aka "Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0100<br>CERT |
| microsoft -- windows_2000<br>microsoft -- windows_2003_server<br>microsoft -- windows_xp | Stack-based buffer overflow in the Word 97 text converter in WordPad in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted Word 97 file that triggers memory corruption, aka "WordPad Word 97 Text Converter Stack Overflow Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0235<br>CERT |
| microsoft -- ie<br>microsoft -- internet_explorer<br>microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_server_2008<br>microsoft -- windows_vista<br>microsoft -- windows_xp | Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008; and WinINet in Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008; allows remote web servers to capture and replay NTLM credentials, and execute arbitrary code, via vectors related to absence of a "credential-reflection protections" opt-in step, aka "Windows HTTP Services Credential Reflection | 2009-04-15 | 9.3 | CVE-2009-0550<br>CERT |

| | | | | |
|---|---|---|---|---|
| | Vulnerability" and "WinINet Credential Reflection Vulnerability." | | | |
| microsoft -- internet_explorer | Microsoft Internet Explorer 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 does not properly handle transition errors in a request for one HTTP document followed by a request for a second HTTP document, which allows remote attackers to execute arbitrary code via vectors involving (1) multiple crafted pages on a web site or (2) a web page with crafted inline content such as banner advertisements, aka "Page Transition Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0551<br>CERT |
| microsoft -- ie | Unspecified vulnerability in Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 on Windows XP SP2 and SP3, and 6 on Windows Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka "Uninitialized Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0552<br>CERT |
| microsoft -- internet_explorer | Microsoft Internet Explorer 5.01 SP4, 6 SP1, 6 and 7 on Windows XP SP2 and SP3, 6 and 7 on Windows Server 2003 SP1 and SP2, 7 on Windows Vista Gold and SP1, and 7 on Windows Server 2008 allows remote attackers to execute arbitrary code via a web page that triggers presence of an object in memory that was (1) not properly initialized or (2) deleted, aka "Uninitialized Memory Corruption Vulnerability." | 2009-04-15 | 9.3 | CVE-2009-0554<br>CERT |
| microsoft -- intelligent_application_gateway_2007 | Multiple stack-based buffer overflows in the Whale Client Components ActiveX control (WhlMgr.dll), as used in Microsoft Intelligent Application Gateway (IAG) before 3.7 SP2, allow remote attackers to execute arbitrary code via long arguments to the (1) CheckForUpdates or (2) UpdateComponents methods. | 2009-04-16 | 9.3 | CVE-2007-2238<br>CERT-VN |
| microsoft -- windows_media_player | Integer overflow in Microsoft Windows Media Player (WMP) 11.0.5721.5260 allows remote attackers to cause a denial of service (application crash) via a crafted .mid file, as demonstrated by crash.mid. | 2009-04-17 | 9.3 | CVE-2009-1331<br>BID<br>MILW0RM |

| | | | | |
|---|---|---|---|---|
| mini-stream -- asx_to_mp3_converter | Stack-based buffer overflow in Mini-stream ASX to MP3 Converter 3.0.0.7 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1324 XF BID MILW0RM MILW0RM SECUNIA |
| mini-stream -- ripper | Stack-based buffer overflow in Mini-stream Ripper 3.0.1.1 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1325 XF BID MILW0RM MILW0RM SECUNIA |
| mini-stream -- rm_downloader | Stack-based buffer overflow in Mini-stream RM Downloader 3.0.0.9 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1326 XF BID MILW0RM MILW0RM SECUNIA |
| mini-stream -- wm_downloader | Stack-based buffer overflow in Mini-stream WM Downloader 3.0.0.9 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1327 XF BID MILW0RM MILW0RM SECUNIA |
| mini-stream -- rm-mp3_converter | Stack-based buffer overflow in Mini-stream RM-MP3 Converter 3.0.0.7 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1328 XF BID MILW0RM MILW0RM SECUNIA |
| mini-stream -- shadow_stream_recorder | Stack-based buffer overflow in Mini-stream Shadow Stream Recorder 3.0.1.7 allows remote attackers to execute arbitrary code via a long URI in a playlist (.m3u) file. | 2009-04-17 | 9.3 | CVE-2009-1329 BID MILW0RM SECUNIA |
| mini-stream -- easy_rm_to_mp3_converter | Stack-based buffer overflow in Easy RM to MP3 Converter allows remote attackers to execute arbitrary code via a long filename in a playlist (.pls) file. | 2009-04-17 | 9.3 | CVE-2009-1330 BID MILW0RM |
| mpg123 -- mpg123 | Integer signedness error in the store_id3_text function in the ID3v2 code in mpg123 before 1.7.2 allows remote attackers to cause a denial of service (out-of-bounds memory access) and possibly execute arbitrary code via an ID3 tag with a negative encoding value. NOTE: some of these details are obtained from third party information. | 2009-04-16 | 10.0 | CVE-2009-1301 VUPEN |
| oracle -- database_9i | Unspecified vulnerability in the Resource Manager component in Oracle Database 9.2.0.8 and 9.2.0.8DV allows remote authenticated users to affect confidentiality, integrity, and | 2009-04-15 | 9.0 | CVE-2009-0979 CERT |

| | | | | |
|---|---|---|---|---|
| | availability via unknown vectors. | | | |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Core RDBMS component in Oracle Database 10.1.0.5, 10.2.0.4, and 11.1.0.6 allows remote authenticated users with the IMP_FULL_DATABASE role to affect confidentiality, integrity, and availability. | 2009-04-15 | 7.1 | CVE-2009-0985<br>CERT |
| oracle -- application_server_10g | Unspecified vulnerability in the OPMN component in Oracle Application Server 10.1.2.3 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 7.5 | CVE-2009-0993<br>CERT |
| oracle -- e-business_suite | The Oracle Applications Framework component in Oracle E-Business Suite 12.0.6 and 11i10CU2 uses default passwords for unspecified "FND Applications Users (not DB users)," which has unknown impact and attack vectors. | 2009-04-15 | 7.5 | CVE-2009-1000<br>CERT |
| oracle -- jrockit | Unspecified vulnerability in the JRockit component in BEA Product Suite R27.6.2 and earlier, with SDK/JRE 1.4.2, JRE/JDK 5, and JRE/JDK 6, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 10.0 | CVE-2009-1006<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 allows remote attackers to affect confidentiality, integrity, and availability, related to IIS. | 2009-04-15 | 10.0 | CVE-2009-1012<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 allows remote authenticated users to affect confidentiality, integrity, and availability, related to IIS. | 2009-04-15 | 8.5 | CVE-2009-1016<br>CERT |
| pgp -- desktop | PGP Desktop before 9.10 allows local users to (1) cause a denial of service (crash) via a crafted IOCTL request to pgpdisk.sys, and (2) cause a denial of service (crash) and execute arbitrary code via a crafted IRP in an IOCTL request to pgpwded.sys. | 2009-04-15 | 7.2 | CVE-2009-0681<br>MISC |
| phpmyadmin -- phpmyadmin | Static code injection vulnerability in the getConfigFile function in setup/lib/ConfigFile.class.php in phpMyAdmin 3.x before 3.1.3.2 allows remote attackers to inject arbitrary PHP code into configuration files. | 2009-04-16 | 7.5 | CVE-2009-1285<br>BID<br>CONFIRM |

| | | | | |
|---|---|---|---|---|
| phpnuke -- php-nuke | SQL injection vulnerability in the Sections module in PHP-Nuke, probably before 8.0, allows remote attackers to execute arbitrary SQL commands via the artid parameter in a printpage action to modules.php. | 2009-04-20 | 7.5 | CVE-2008-6728<br>BUGTRAQ<br>OSVDB<br>BUGTRAQ |
| sap -- sap_gui | Insecure method vulnerability in the KWEdit ActiveX control in SAP GUI 6.40 Patch 29 (KWEDIT.DLL 6400.1.1.41) and 7.10 Patch 5 (KWEDIT.DLL 7100.1.1.43) allows remote attackers to (1) overwrite arbitrary files via the SaveDocumentAs method or (2) read or execute arbitrary files via the OpenDocument method. | 2009-04-16 | 9.3 | CVE-2008-4830<br>VUPEN |
| thomas_waggershauser -- air_filemanager | Unspecified vulnerability in Frontend Filemanager (air_filemanager) 0.6.1 and earlier extension for TYPO3 allows remote attackers to execute arbitrary commands via unknown vectors. | 2009-04-10 | 7.5 | CVE-2008-6685<br>CONFIRM |
| turnkeyforms -- entertainment_portal | TurnkeyForms Entertainment Portal 2.0 allows remote attackers to bypass authentication and gain administrative access by setting the adminLogged cookie to Administrator. | 2009-04-14 | 7.5 | CVE-2008-6723<br>XF<br>BID<br>MILW0RM<br>SECUNIA<br>OSVDB |
| vmware -- ace<br>vmware -- esx<br>vmware -- esxi<br>vmware -- fusion<br>vmware -- player<br>vmware -- server<br>vmware -- workstation | Unspecified vulnerability in the virtual machine display function in VMware Workstation 6.5.1 and earlier; VMware Player 2.5.1 and earlier; VMware ACE 2.5.1 and earlier; VMware Server 1.x before 1.0.9 build 156507 and 2.x before 2.0.1 build 156745; VMware Fusion before 2.0.4 build 159196; VMware ESXi 3.5; and VMware ESX 3.0.2, 3.0.3, and 3.5 allows guest OS users to execute arbitrary code on the host OS via unknown vectors, a different vulnerability than CVE-2008-4916. | 2009-04-13 | 10.0 | CVE-2009-1244<br>BID<br>MLIST |
| webfileexplorer -- web_file_explorer | body.asp in Web File Explorer 3.1 allows remote attackers to create arbitrary files and execute arbitrary code via the savefile action with a file parameter containing a filename that has an executable extension. | 2009-04-16 | 10.0 | CVE-2009-1314<br>MILW0RM |
| webfileexplorer -- web_file_explorer | SQL injection vulnerability in body.asp in Web File Explorer 3.1 allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2009-04-17 | 7.5 | CVE-2009-1323<br>XF<br>BID<br>MILW0RM<br>SECUNIA |
| xecms -- xecms | admin.php in xeCMS 1.0.0 RC2 and earlier allows remote attackers to bypass authentication and access | 2009-04-10 | 7.5 | CVE-2008-6714<br>XF |

| | | | | |
|---|---|---|---|---|
| | the admin panel by setting the xecms_username cookie. | 10 | | BID<br>MILW0RM |

Back to top

**Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)**

| Primary Vendor -- Product | Description | Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| abk-soft -- ablespace | Multiple cross-site scripting (XSS) vulnerabilities in AbleSpace 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) gid parameter to groups_profile.php, (2) cat_id and (3) razd_id parameters to adv_cat.php, and the (4) URL to blogs_full.php. | 2009-04-17 | 4.3 | CVE-2009-1315<br>BID<br>BUGTRAQ<br>MILW0RM<br>MISC |
| apache -- geronimo | Multiple cross-site scripting (XSS) vulnerabilities in the web administration console in Apache Geronimo Application Server 2.1 through 2.1.3 allow remote attackers to inject arbitrary web script or HTML via the (1) name, (2) ip, (3) username, or (4) description parameter to console/portal/Server/Monitoring; or (5) the PATH_INFO to the default URI under console/portal/. | 2009-04-17 | 4.3 | CVE-2009-0038<br>CONFIRM<br>CONFIRM |
| apache -- geronimo | Multiple cross-site request forgery (CSRF) vulnerabilities in the web administration console in Apache Geronimo Application Server 2.1 through 2.1.3 allow remote attackers to hijack the authentication of administrators for requests that (1) change the web administration password, (2) upload applications, and perform unspecified other administrative actions, as demonstrated by (3) a Shutdown request to console/portal//Server/Shutdown. | 2009-04-17 | 6.8 | CVE-2009-0039<br>BID<br>BUGTRAQ<br>CONFIRM<br>CONFIRM<br>MISC |
| aquacms -- aqua_cms | Multiple SQL injection vulnerabilities in Aqua CMS 1.1, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) userSID cookie parameter to droplets/functions/base.php and the (2) username parameter to admin/index.php. | 2009-04-17 | 6.8 | CVE-2009-1317<br>BID<br>MILW0RM<br>SECUNIA |
| chcounter -- chcounter | Multiple SQL injection vulnerabilities in stats/index.php in chCounter 3.1.3 allow remote attackers to execute arbitrary SQL commands via (1) the login_name parameter (aka the username field) or (2) the login_pw parameter (aka the password field). | 2009-04-20 | 6.8 | CVE-2009-1347<br>BID<br>MILW0RM<br>SECUNIA |
| china-on-site -- flexphplink | Multiple SQL injection vulnerabilities in admin/usercheck.php in FlexPHPLink Pro 0.0.6 and 0.0.7, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via (1) the checkuser parameter (aka username field), or (2) the checkpass parameter (aka password field), to admin/index.php. | 2009-04-20 | 6.8 | CVE-2008-6730<br>XF<br>OSVDB<br>MILW0RM<br>SECUNIA |
| cisco -- subscriber_edge_services_manager | Cross-site scripting (XSS) vulnerability in Cisco Subscriber Edge Services Manager (SESM) allows remote attackers to inject arbitrary web script or HTML via the URI. NOTE: some of these details are obtained from third party information. | 2009-04-13 | 4.3 | CVE-2009-1287<br>MISC<br>BID<br>SECTRACK |
| cmscout -- cmscout | Multiple SQL injection vulnerabilities in CMScout 2.06 allow remote authenticated users to execute arbitrary SQL commands via the id parameter to (1) index.php in a mythings page (mythings.php) and (2) the users page in admin.php. | 2009-04-17 | 6.0 | CVE-2008-6725<br>XF<br>BID<br>MILW0RM<br>CONFIRM<br>SECUNIA<br>OSVDB |
| cmscout -- cmscout | Multiple directory traversal vulnerabilities in CMScout 2.06, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the bit parameter to (1) admin.php and (2) index.php, different vectors than CVE-2008-3415. | 2009-04-17 | 6.0 | CVE-2008-6726<br>XF<br>CONFIRM |
| david_cadu -- dcdgooglemap | Cross-site scripting (XSS) vulnerability in DCD GoogleMap (dcdgooglemap) 1.1.0 and earlier extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors. | 2009-04-10 | 4.3 | CVE-2008-6687<br>CONFIRM |

| | | | | |
|---|---|---|---|---|
| drupal -- cck_comment_reference | Cross-site scripting (XSS) vulnerability in the CCK comment reference module 6.x before 6.x-1.2, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via certain comment titles associated with a node edit form. | 2009-04-20 | 4.3 | CVE-2009-1342<br>VUPEN<br>CONFIRM |
| drupal -- print | Cross-site scripting (XSS) vulnerability in the Print (aka Printer, e-mail and PDF versions) module 5.x before 5.x-4.5 and 6.x before 6.x-1.5, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via content titles. | 2009-04-20 | 4.3 | CVE-2009-1343<br>VUPEN<br>BID<br>CONFIRM |
| drupal -- localization_client | Cross-site scripting (XSS) vulnerability in the Localization client module 5.x before 5.x-1.2 and 6.x before 6.x-1.7, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via input to the translation functionality. | 2009-04-20 | 4.3 | CVE-2009-1344<br>VUPEN<br>BID<br>CONFIRM |
| hp -- procurve_manager | Unspecified vulnerability in HP ProCurve Manager and HP ProCurve Manager Plus 2.3 and earlier allows remote attackers to obtain sensitive information from the ProCurve Manager server via unknown attack vectors. | 2009-04-15 | 5.0 | CVE-2007-4514<br>XF<br>HP<br>HP |
| hp -- deskjet_6840 | Cross-site scripting (XSS) vulnerability in refresh_rate.htm in the web interface on the HP Deskjet 6840 printer with firmware XF1M131A allows remote attackers to inject arbitrary web script or HTML via the POST request body. | 2009-04-17 | 4.3 | CVE-2009-1333<br>XF<br>BUGTRAQ |
| humayun_shabbir_bhutta -- asp_product_catalog | Cross-site scripting (XSS) vulnerability in search.asp in ASP Product Catalog 1.0 allows remote attackers to inject arbitrary web script or HTML via the keywords parameter. | 2009-04-17 | 4.3 | CVE-2009-1321<br>XF<br>BID<br>MILW0RM |
| humayun_shabbir_bhutta -- asp_product_catalog | ASP Product Catalog 1.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing user credentials via a direct request for database/aspProductCatalog.mdb. | 2009-04-17 | 5.0 | CVE-2009-1322<br>XF<br>MILW0RM |
| ibm -- lotus_domino | The IMAP task in the server in IBM Lotus Domino 8.0.2 before FP1 IF1 and 8.5 before IF3 allows remote attackers to cause a denial of service (daemon crash) via a MIME e-mail message with RFC822 attachments (aka blobs) containing malformed root entities. | 2009-04-13 | 5.0 | CVE-2009-1286<br>CONFIRM<br>CONFIRM |
| ibm -- advanced_management_module<br>ibm -- bladecenter | Multiple cross-site scripting (XSS) vulnerabilities in the Advanced Management Module (AMM) on the IBM BladeCenter, including the BladeCenter H with BPET36H 54, allow remote attackers to inject arbitrary web script or HTML via (1) the username in a login action or (2) the PATH parameter to private/file_management.ssi in the File manager. | 2009-04-13 | 4.3 | CVE-2009-1288<br>BID<br>BUGTRAQ<br>MISC<br>SECTRACK<br>OSVDB<br>OSVDB |
| ibm -- advanced_management_module<br>ibm -- bladecenter | private/login.ssi in the Advanced Management Module (AMM) on the IBM BladeCenter, including the BladeCenter H with BPET36H 54, allows remote attackers to discover the access roles and scopes of arbitrary user accounts via a modified WEBINDEX parameter. | 2009-04-13 | 4.0 | CVE-2009-1289<br>BID<br>BUGTRAQ<br>MISC<br>SECTRACK<br>OSVDB |
| ibm -- advanced_management_module<br>ibm -- bladecenter | Multiple cross-site request forgery (CSRF) vulnerabilities in the web administration interface in the Advanced Management Module (AMM) on the IBM BladeCenter, including the BladeCenter H with BPET36H 54, allow remote attackers to hijack the authentication of administrators, as demonstrated by a power-off request to the private/blade_power_action script. | 2009-04-13 | 6.8 | CVE-2009-1290<br>BID<br>BUGTRAQ<br>MISC<br>SECTRACK<br>OSVDB |
| | Cross-site scripting (XSS) vulnerability in login/FilepathLogin.html in | | | CVE-2009-1334<br>XF<br>VUPEN |

| | | | | |
|---|---|---|---|---|
| ibm -- tivoli_continuous_data_protection_for_files | IBM Tivoli Continuous Data Protection (CDP) for Files 3.1.4.0 allows remote attackers to inject arbitrary web script or HTML via the reason parameter. | 2009-04-17 | 4.3 | VUPEN BID OSVDB MISC SECTRACK SECUNIA |
| jamroom -- jamroom | Directory traversal vulnerability in index.php in Jamroom 3.1.2, 3.2.3 through 3.2.6, 4.0.2, and possibly other versions before 3.4.0 allows remote attackers to include arbitrary files via directory traversal sequences in the t parameter. | 2009-04-17 | 6.5 | CVE-2009-1318 XF BID MILW0RM CONFIRM |
| kernel -- linux-pam | Linux-PAM before 1.0.4 does not enforce the minimum password age (MINDAYS) as specified in /etc/shadow, which allows local users to bypass intended security policy and change their passwords sooner than specified. | 2009-04-16 | 4.6 | CVE-2009-0579 FEDORA CONFIRM |
| liferay -- liferay_enterprise_portal novell -- teaming | Multiple cross-site scripting (XSS) vulnerabilities in web/guest/home in the Liferay 4.3.0 portal in Novell Teaming 1.0 through SP3 (1.0.3) allow remote attackers to inject arbitrary web script or HTML via the (1) p_p_state or (2) p_p_mode parameters. | 2009-04-16 | 4.3 | CVE-2009-1294 CONFIRM |
| microsoft -- forefront_threat_management_gateway microsoft -- internet_security_and_acceleration_server | The firewall engine in Microsoft Forefront Threat Management Gateway, Medium Business Edition (TMG MBE); and Internet Security and Acceleration (ISA) Server 2004 SP3, 2006, 2006 Supportability Update, and 2006 SP1; does not properly manage the session state of web listeners, which allows remote attackers to cause a denial of service (many stale sessions) via crafted packets, aka "Web Proxy TCP State Limited Denial of Service Vulnerability." | 2009-04-15 | 5.0 | CVE-2009-0077 CERT |
| microsoft -- windows_server_2003 microsoft -- windows_xp | The RPCSS service in Microsoft Windows XP SP2 and SP3 and Server 2003 SP1 and SP2 does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by accessing the resources of one of the processes, aka "Windows RPCSS Service Isolation Vulnerability." | 2009-04-15 | 6.9 | CVE-2009-0079 CERT |
| microsoft -- windows_server microsoft -- windows_vista | The ThreadPool class in Windows Vista Gold and SP1, and Server 2008, does not properly implement isolation among a set of distinct processes that (1) all run under the NetworkService account or (2) all run under the LocalService account, which allows local users to gain privileges by leveraging incorrect thread ACLs to access the resources of one of the processes, aka "Windows Thread Pool ACL Weakness Vulnerability." | 2009-04-15 | 6.9 | CVE-2009-0080 CERT |
| microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp | Windows HTTP Services (aka WinHTTP) in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, and Vista Gold allows remote web servers to impersonate arbitrary https web sites by using DNS spoofing to "forward a connection" to a different https web site that has a valid certificate matching its own domain name, but not a certificate matching the domain name of the host requested by the user, aka "Windows HTTP Services Certificate Name Mismatch Vulnerability." | 2009-04-15 | 5.8 | CVE-2009-0089 CERT |
| microsoft -- forefront_threat_management_gateway microsoft -- internet_security_and_acceleration_server | Cross-site scripting (XSS) vulnerability in cookieauth.dll in the HTML forms authentication component in Microsoft Forefront Threat Management Gateway, Medium Business Edition (TMG MBE); and Internet Security and Acceleration (ISA) Server 2006, 2006 Supportability Update, and 2006 SP1; allows remote attackers to inject arbitrary web script or HTML via "authentication input" to this component, aka "Cross-Site Scripting Vulnerability." | 2009-04-15 | 4.3 | CVE-2009-0237 CERT |
| microsoft -- ie | Microsoft Internet Explorer 7 and 8 on Windows XP and Vista allows remote attackers to cause a denial of service (application hang) via a large document composed of unprintable characters, aka MSRC 9011jr. | 2009-04-17 | 4.3 | CVE-2009-1335 BUGTRAQ |
| myupb -- upb | Cross-site scripting (XSS) vulnerability in Ultimate PHP Board (UPB) 2.2.2, 2.2.1, and earlier 2.x versions allows remote attackers to inject arbitrary web script or HTML via the User-Agent HTTP header. | 2009-04-20 | 4.3 | CVE-2008-6727 XF BID MILW0RM SECUNIA |

| | | | | |
|---|---|---|---|---|
| | | | | OSVDB |
| novell -- teaming | The web login functionality (c/portal/login) in Novell Teaming 1.0 through SP3 (1.0.3) generates different error messages depending on whether the username is valid or invalid, which makes it easier for remote attackers to enumerate usernames. | 2009-04-16 | 5.0 | CVE-2009-1293 CONFIRM |
| ntp -- ntp | Stack-based buffer overflow in the cookedprint function in ntpq/ntpq.c in ntpq in NTP before 4.2.4p7-RC2 allows remote NTP servers to execute arbitrary code via a crafted response. | 2009-04-14 | 6.8 | CVE-2009-0159 CONFIRM BID |
| oracle -- database_10g<br>oracle -- database_11g<br>oracle -- database_9i | Unspecified vulnerability in the Workspace Manager component in Oracle Database 11.1.0.6, 11.1.0.7, 10.2.0.3, 10.2.0.4, 10.1.0.5, 9.2.0.8, and 9.2.0.8DV allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 6.5 | CVE-2009-0972 CERT |
| oracle -- database_10g | Unspecified vulnerability in the Cluster Ready Services component in Oracle Database 10.1.0.5 allows remote attackers to affect availability via unknown vectors. | 2009-04-15 | 5.0 | CVE-2009-0973 CERT |
| oracle -- application_server_10g | Unspecified vulnerability in the Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors. | 2009-04-15 | 4.3 | CVE-2009-0974 CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Workspace Manager component in Oracle Database 10.2.0.4 and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-0975 CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Workspace Manager component in Oracle Database 10.2.0.4 and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to LTADM. | 2009-04-15 | 5.5 | CVE-2009-0976 CERT |
| oracle -- database_10g<br>oracle -- database_9i | Unspecified vulnerability in the Advanced Queuing component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, and 10.2.0.3 allows remote authenticated users to affect confidentiality and integrity, related to DBMS_AQIN. | 2009-04-15 | 5.5 | CVE-2009-0977 CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Workspace Manager component in Oracle Database 10.2.0.4 and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-0978 CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the SQLX Functions component in Oracle Database 10.2.0.3 and 11.1.0.6 allows remote authenticated users to affect integrity and availability, related to AGGXQIMP. | 2009-04-15 | 5.5 | CVE-2009-0980 CERT |
| oracle -- database_11g | Unspecified vulnerability in the Application Express component in Oracle Database 11.1.0.7 allows remote authenticated users to affect confidentiality, related to APEX. | 2009-04-15 | 4.0 | CVE-2009-0981 CERT |
| oracle -- jd_edwards_enterpriseone<br>oracle -- peoplesoft_enterprise | Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.49.19 allows remote authenticated users to affect integrity via unknown vectors. | 2009-04-15 | 4.0 | CVE-2009-0982 CERT |
| oracle -- application_server_10g | Unspecified vulnerability in the Portal component in Oracle Application Server 10.1.2.3 and 10.1.4.2 allows remote attackers to affect integrity via unknown vectors, a different vulnerability than CVE-2009-0974. | 2009-04-15 | 4.3 | CVE-2009-0983 CERT |
| oracle -- database_10g<br>oracle -- database_11g<br>oracle -- database_9i | Unspecified vulnerability in the Database Vault component in Oracle Database 9.2.0.8DV, 10.2.0.4, and 11.1.0.6 allows remote authenticated users to affect confidentiality and integrity, related to DBMS_SYS_SQL. | 2009-04-15 | 5.5 | CVE-2009-0984 CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Workspace Manager component in Oracle Database 10.2.0.4 and 11.1.0.6 allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 5.4 | CVE-2009-0986 CERT |
| oracle -- application_server<br>oracle -- application_server_10g | Unspecified vulnerability in the BI Publisher component in Oracle Application Server 5.6.2, 10.1.3.2.1, and 10.1.3.3.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-0989 CERT |
| oracle -- application_server<br>oracle -- application_server_10g | Unspecified vulnerability in the BI Publisher component in Oracle Application Server 5.6.2, 10.1.3.2.1, and 10.1.3.3.3 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-0990 CERT |

| | | | | |
|---|---|---|---|---|
| oracle -- database_10g<br>oracle -- database_11g<br>oracle -- database_9i | Unspecified vulnerability in the Listener component in Oracle Database 9.2.0.8, 9.2.0.8DV, 10.1.0.5, 10.2.0.4, and 11.1.0.7 allows remote attackers to affect availability via unknown vectors. | 2009-04-15 | 5.0 | CVE-2009-0991<br>CERT |
| oracle -- database_10g<br>oracle -- database_11g | Unspecified vulnerability in the Advanced Queuing component in Oracle Database 10.1.0.5, 10.2.0.4, and 11.1.0.7 allows remote authenticated users to affect confidentiality and integrity, related to DBMS_AQIN. | 2009-04-15 | 5.5 | CVE-2009-0992<br>CERT |
| oracle -- application_server<br>oracle -- application_server_10g | Unspecified vulnerability in the BI Publisher component in Oracle Application Server 5.6.2, 10.1.3.2.1, 10.1.3.3.3, and 10.1.3.4 allows remote authenticated users to affect confidentiality via unknown vectors. | 2009-04-15 | 4.0 | CVE-2009-0994<br>CERT |
| oracle -- e-business_suite<br>oracle -- e-business_suite_12 | Unspecified vulnerability in the Oracle Applications Framework component in Oracle E-Business Suite 12.0.6 and 11i10CU2 allows remote attackers to affect integrity via unknown vectors. | 2009-04-15 | 4.3 | CVE-2009-0995<br>CERT |
| oracle -- application_server_10g | Unspecified vulnerability in the BI Publisher component in Oracle Application Server 10.1.3.2.1, 10.1.3.3.3, and 10.1.3.4 allows remote authenticated users to affect confidentiality via unknown vectors. | 2009-04-15 | 4.0 | CVE-2009-0996<br>CERT |
| oracle -- database_11g | Unspecified vulnerability in the Database Vault component in Oracle Database 11.1.0.6 allows remote authenticated users to affect confidentiality, related to DBMS_SYS_SQL. | 2009-04-15 | 4.0 | CVE-2009-0997<br>CERT |
| oracle -- jd_edwards_enterpriseone<br>oracle -- peoplesoft_enterprise | Unspecified vulnerability in the PeopleSoft Enterprise HRMS - eBenefits component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.9.18 and 9.0.8 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-0998<br>CERT |
| oracle -- e-business_suite | Unspecified vulnerability in the Oracle Application Object Library component in Oracle E-Business Suite 12.0.6 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 6.8 | CVE-2009-0999<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Portal component in BEA Product Suite 8.1 SP6 allows remote authenticated users to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.5 | CVE-2009-1001<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, 9.0, 8.1 SP6, and 7.0 SP7 allows remote attackers to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.8 | CVE-2009-1002<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3, 10.0 MP1, 9.2 MP3, 9.1, and 9.0 allows remote attackers to affect integrity via unknown vectors. | 2009-04-15 | 5.0 | CVE-2009-1003<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the WebLogic Server component in BEA Product Suite 10.3 allows remote attackers to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 4.0 | CVE-2009-1004<br>CERT |
| oracle -- bea_product_suite | Unspecified vulnerability in the Oracle Data Service Integrator (AquaLogic Data Services Platform) component in BEA Product Suite 10.3.0, 3.2, 3.0.1, and 3.0 allows local users to affect confidentiality, integrity, and availability via unknown vectors. | 2009-04-15 | 4.1 | CVE-2009-1005<br>CERT |
| oracle -- application_server | Unspecified vulnerability in the Outside In Technology component in Oracle Application Server 8.2.2 and 8.3.0 allows local users to affect confidentiality, integrity, and availability, related to HTML. | 2009-04-15 | 4.4 | CVE-2009-1008<br>CERT |
| oracle -- application_server | Unspecified vulnerability in the Outside In Technology component in Oracle Application Server 8.1.9 allows local users to affect confidentiality, integrity, and availability, related to HTML. | 2009-04-15 | 4.4 | CVE-2009-1009<br>CERT |
| oracle -- application_server | Unspecified vulnerability in the Outside In Technology component in Oracle Application Server 8.2.2 and 8.3.0 allows local users to affect confidentiality, integrity, and availability, related to HTML. | 2009-04-15 | 4.4 | CVE-2009-1010<br>CERT |
| oracle -- application_server | Unspecified vulnerability in the Outside In Technology component in Oracle Application Server 8.2.2 and 8.3.0 allows local users to affect confidentiality, integrity, and availability, related to HTML. | 2009-04-15 | 4.4 | CVE-2009-1011<br>CERT |
| oracle -- jd_edwards_enterpriseone<br>oracle -- peoplesoft_enterprise | Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.49.19 allows remote attackers to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 6.4 | CVE-2009-1013<br>CERT |
| | Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools | | | CVE-2009 |

| | | | | |
|---|---|---|---|---|
| oracle -- jd_edwards_enterpriseone<br>oracle -- peoplesoft_enterprise | component in Oracle PeopleSoft Enterprise and JD Edwards EnterpriseOne 8.49.19 allows remote attackers to affect confidentiality and integrity via unknown vectors. | 2009-04-15 | 5.8 | CVE-2009-1014<br>CERT |
| oracle -- application_server<br>oracle -- application_server_10g | Unspecified vulnerability in the BI Publisher component in Oracle Application Server 5.6.2, 10.1.3.2.1, 10.1.3.3.3, and 10.1.3.4 allows remote authenticated users to affect confidentiality via unknown vectors. | 2009-04-15 | 4.0 | CVE-2009-1017<br>CERT |
| patrick_matthai -- pnopaste | Cross-site scripting (XSS) vulnerability in index.pl in Perl Nopaste 1.0 allows remote attackers to inject arbitrary web script or HTML via the language parameter. NOTE: some of these details are obtained from third party information. | 2009-04-17 | 4.3 | CVE-2008-6724<br>BID<br>CONFIRM |
| phpmotion -- phpmotion | Multiple cross-site request forgery (CSRF) vulnerabilities in password.php in PHPmotion 2.1 and earlier allow remote attackers to hijack the authentication of arbitrary users for requests that modify an account via the (1) password or (2) email_address parameter. | 2009-04-20 | 6.8 | CVE-2008-6729<br>XF<br>MILW0RM<br>SECUNIA<br>OSVDB |
| sun -- openjdk | Integer overflow in the PulseAudioTargetDataL class in src/java/org/classpath/icedtea/pulseaudio/PulseAudioTargetDataLine.java in Pulse-Java, as used in OpenJDK 1.6.0.0 and other products, allows remote attackers to cause a denial of service (applet crash) via a crafted Pulse Audio source data line. | 2009-04-13 | 5.0 | CVE-2009-0794<br>FEDORA<br>FEDORA<br>CONFIRM<br>VUPEN<br>SECUNIA<br>MLIST |
| sun -- java_system_directory_server | The Online Help feature in Sun Java System Directory Server 5.2 and Enterprise Edition 5 allows remote attackers to determine the existence of files and directories, and possibly obtain partial contents of files, via unspecified vectors. | 2009-04-17 | 5.0 | CVE-2009-1332<br>BID<br>SUNALERT<br>SECUNIA |
| wireshark -- wireshark | Unspecified vulnerability in the LDAP dissector in Wireshark 0.99.2 through 1.0.6, when running on Windows, allows remote attackers to cause a denial of service (crash) via unknown attack vectors. | 2009-04-13 | 5.0 | CVE-2009-1267<br>CONFIRM |
| wireshark -- wireshark | The Check Point High-Availability Protocol (CPHAP) dissector in Wireshark 0.9.6 through 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted FWHA_MY_STATE packet. | 2009-04-13 | 4.3 | CVE-2009-1268<br>MISC<br>XF<br>CONFIRM<br>SECTRACK<br>BID<br>MANDRIVA |
| wireshark -- wireshark | Unspecified vulnerability in Wireshark 0.99.6 through 1.0.6 allows remote attackers to cause a denial of service (crash) via a crafted Tektronix .rf5 file. | 2009-04-13 | 5.0 | CVE-2009-1269<br>XF<br>CONFIRM<br>SECTRACK<br>BID<br>MANDRIVA |
| yourfreeworld -- apartment_search_script | Cross-site scripting (XSS) vulnerability in listtest.php in Apartment Search Script allows remote attackers to inject arbitrary web script or HTML via the r parameter. | 2009-04-10 | 4.3 | CVE-2008-6683<br>XF<br>BID<br>MILW0RM |
| zazzle -- store_builder | Multiple cross-site scripting (XSS) vulnerabilities in include/zstore.php in Zazzle Store Builder 1.0.2 allow remote attackers to inject arbitrary web script or HTML via the (1) gridPage and (2) gridSort parameters. NOTE: some of these details are obtained from third party information. | 2009-04-17 | 4.3 | CVE-2009-1320<br>BID<br>SECUNIA<br>MISC |

Back to top

| Low Vulnerabilities (CVSS Score: 0.0 .. 3.9) | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |

| | | | | |
|---|---|---|---|---|
| ibm -- rational_clearcase | UCM-CQ in IBM Rational ClearCase 7.0.0.x before 7.0.0.5, 7.0.1.x before 7.0.1.4, and 7.1.x before 7.1.0.1 on Linux and AIX places a username and password on the command line, which allows local users to obtain credentials by listing the process. | 2009-04-14 | 2.1 | CVE-2009-1292<br>AIXAPAR |
| kernel -- udev | Buffer overflow in the util_path_encode function in udev/lib/libudev-util.c in udev before 1.4.1 allows local users to cause a denial of service (service outage) via vectors that trigger a call with crafted arguments. | 2009-04-17 | 2.1 | CVE-2009-1186<br>MISC<br>CONFIRM<br>UBUNTU<br>BID<br>DEBIAN<br>SECUNIA<br>SECUNIA<br>SECUNIA<br>CONFIRM |
| novell -- access_manager | Novell Access Manager 3 SP4 does not properly expire X.509 certificate sessions, which allows physically proximate attackers to obtain a logged-in session by using a victim's web-browser process that continues to send the original and valid SSL sessionID, related to inability of Apache Tomcat to clear entries from its SSL cache. | 2009-04-14 | 1.9 | CVE-2008-6722<br>VUPEN<br>CONFIRM<br>SECUNIA<br>OSVDB |
| oracle -- database_11g | Unspecified vulnerability in the Password Policy component in Oracle Database 11.1.0.6 allows remote authenticated users to affect confidentiality via unknown vectors. | 2009-04-15 | 2.1 | CVE-2009-0988<br>CERT |

Back to top