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** | **Published** | **CVSS Score** | **Source & Patch Info** |
| 6rbscript -- 6rbscript | SQL injection vulnerability in section.php in 6rbScript 3.3 allows remote attackers to execute arbitrary SQL commands via the singerid parameter in a singers action. | 2009-03-13 | 7.5 | CVE-2008-6454 BID MILW0RM |
| akirapowered -- image_gallery | SQL injection vulnerability in image_gallery.php in the Akira Powered Image Gallery (image_gallery) plugin for e107 allows remote attackers to execute arbitrary SQL commands via the image parameter in an image-detail action. | 2009-03-13 | 7.5 | CVE-2008-6466 BID MILW0RM |
| apple -- itunes | Apple iTunes before 8.1 does not properly inform the user about the origin of an authentication request, which makes it easier for remote podcast servers to trick a user into providing a username and password when subscribing to a crafted podcast. | 2009-03-14 | 7.1 | CVE-2009-0143 CONFIRM APPLE |

| | | | | |
|---|---|---|---|---|
| baidu -- baidu_hi | Stack-based buffer overflow in CSTransfer.dll in Baidu Hi IM might allow remote attackers to execute arbitrary code via a crafted packet, probably related to an improper length value. | 2009-03-09 | 9.3 | CVE-2008-6444 XF BID BUGTRAQ |
| blueriver -- sava_cms | SQL injection vulnerability in index.cfm in Blue River Interactive Group Sava CMS before 5.0.122 allows remote attackers to execute arbitrary SQL commands via the LinkServID parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2009-03-06 | 7.5 | CVE-2008-6434 BID SECUNIA |
| cisco -- unified_communications_manager | The IP Phone Personal Address Book (PAB) Synchronizer feature in Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 4.1, 4.2 before 4.2(3)SR4b, 4.3 before 4.3(2)SR1b, 5.x before 5.1(3e), 6.x before 6.1(3), and 7.0 before 7.0(2) sends privileged directory-service account credentials to the client in cleartext, which allows remote attackers to modify the CUCM configuration and perform other privileged actions by intercepting these credentials, and then using them in requests unrelated to the intended synchronization task, as demonstrated by (1) DC Directory account credentials in CUCM 4.x and (2) TabSyncSysUser account credentials in CUCM 5.x through 7.x. | 2009-03-12 | 9.0 | CVE-2009-0632 VUPEN CISCO |
| dieselscripts -- diesel_job_site | SQL injection vulnerability in jobs/jobseekers/job-info.php in Diesel Job Site allows remote attackers to execute arbitrary SQL commands via the job_id parameter. | 2009-03-13 | 7.5 | CVE-2008-6467 BID MILW0RM |
| dieselscripts -- diesel_pay | SQL injection vulnerability in index.php in Diesel Pay allows remote attackers to execute arbitrary SQL commands via the area parameter in a browse action. | 2009-03-13 | 7.5 | CVE-2008-6468 BID MILW0RM |
| | SQL injection vulnerability in the FE address edit for tt_address & direct_mail | | | CVE-2008- |

| | | | | |
|---|---|---|---|---|
| dieter_mayer -- fe_address_edit | address edit for tt_address & direct mail (dmaddredit) extension 0.4.0 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | 6458 XF BID CONFIRM |
| e107coders -- macguru_blog_engine_plugin | SQL injection vulnerability in macgurublog_menu/macgurublog.php in the MacGuru BLOG Engine plugin 2.2 for e107 allows remote attackers to execute arbitrary SQL commands via the uid parameter, a different vector than CVE-2008-2455. | 2009-03-06 | 7.5 | CVE-2008-6438 BID MILW0RM |
| epicgames -- unreal_engine | Format string vulnerability in the Epic Games Unreal engine client, as used in multiple games, allows remote servers to execute arbitrary code via (1) the CLASS parameter in a DLMGR command, (2) a malformed package (PKG), and possibly (3) the LEVEL parameter in a WELCOME command. | 2009-03-09 | 9.3 | CVE-2008-6441 XF BID BUGTRAQ OSVDB OSVDB SECUNIA FULLDISC MISC |
| foxit -- reader3.0 | Stack-based buffer overflow in Foxit Reader 3.0 before Build 1506, including 1120 and 1301, allows remote attackers to execute arbitrary code via a long (1) relative path or (2) absolute path in the filename argument in an action, as demonstrated by the "Open/Execute a file" action. | 2009-03-10 | 10.0 | CVE-2009-0837 XF VUPEN BID CONFIRM MISC SECUNIA |
| foxitsoftware -- foxit_reader | Foxit Reader 2.3 before Build 3902 and 3.0 before Build 1506, including 3.0.2009.1301, does not properly handle a JBIG2 symbol dictionary segment with zero new symbols, which allows remote attackers to execute arbitrary code via a crafted PDF file that triggers a dereference of an uninitialized memory location. | 2009-03-10 | 9.3 | CVE-2009-0191 VUPEN CONFIRM |
| fr.simon_rundell -- ste_prayer2 | SQL injection vulnerability in the Random Prayer 2 (ste_prayer2) extension before 0.0.3 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6461 CONFIRM |
| | SQL injection vulnerability in the | | | |

| | | | | |
|---|---|---|---|---|
| fr.simon_rundell -- pd_churchsearch | Diocese of Portsmouth Church Search (pd_churchsearch) extension before 0.1.1, and 0.2.10 and earlier 0.2.x versions, an extension for TYPO3, allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6463 BID CONFIRM |
| geniuscyber -- maxsite | Static code injection vulnerability in the Guestbook component in CMS MAXSITE allows remote attackers to inject arbitrary PHP code into the guestbook via the message parameter. | 2009-03-09 | 7.5 | CVE-2008-6446 XF BID MILW0RM |
| geovision -- livex_activex_control | Directory traversal vulnerability in the SnapShotToFile method in the GeoVision LiveX (aka LiveX_v8200) ActiveX control 8.1.2 and 8.2.0 in LIVEX_~1.OCX allows remote attackers to create or overwrite arbitrary files via a .. (dot dot) in the argument, possibly involving the PlayX and SnapShotX methods. | 2009-03-10 | 8.8 | CVE-2009-0865 XF BID SECUNIA MILW0RM |
| hp -- wmi_mapper | Unspecified vulnerability in WMI Mapper for HP Systems Insight Manager before 2.5.2.0 allows local users to gain privileges via unknown vectors. | 2009-03-11 | 7.2 | CVE-2009-0712 HP |
| ibm -- tivoli_storage_manager_hsm | Buffer overflow in the client in IBM Tivoli Storage Manager (TSM) HSM 5.3.2.0 through 5.3.5.0, 5.4.0.0 through 5.4.2.5, and 5.5.0.0 through 5.5.1.4 on Windows allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors. | 2009-03-10 | 10.0 | CVE-2009-0869 BID CONFIRM |
| ibm -- tivoli_storage_manager ibm -- tivoli_storage_manager_express | Heap-based buffer overflow in adsmdll.dll 5.3.7.7296, as used by the daemon (dsmsvc.exe) in IBM Tivoli Storage Manager (TSM) Express 5.4.0.0 through 5.4.4.0, 5.3 including 5.3.7.3, and 5.2 allows remote attackers to execute arbitrary code via a crafted length value. | 2009-03-11 | 10.0 | CVE-2008-4563 CONFIRM |
| josema_enzo -- isiajax | SQL injection vulnerability in ejemplo/paises.php in isiAJAX 1 allows remote attackers to execute arbitrary | 2009-03-12 | 7.5 | CVE-2009-0881 XF |

| | | | | |
|---|---|---|---|---|
| | SQL commands via the id parameter. | | | MILW0RM |
| jportal -- jportal | SQL injection vulnerability in humor.php in jPORTAL 2 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: this might overlap CVE-2004-2036 or CVE-2005-3509. | 2009-03-13 | 7.5 | CVE-2008-6451 BID MILW0RM |
| kernel -- linux | The icmp_send function in net/ipv4/icmp.c in the Linux kernel before 2.6.25, when configured as a router with a REJECT route, does not properly manage the Protocol Independent Destination Cache (aka DST) in some situations involving transmission of an ICMP Host Unreachable message, which allows remote attackers to cause a denial of service (connectivity outage) by sending a large series of packets to many destination IP addresses within this REJECT route, related to an "rt_cache leak." | 2009-03-12 | 7.1 | CVE-2009-0778 CONFIRM XF BID CONFIRM MLIST CONFIRM |
| kurt_gusbeth -- myquizpoll | SQL injection vulnerability in the My quiz and poll (myquizpoll) extension before 0.1.4 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6462 CONFIRM |
| martin_helmich -- hbook | SQL injection vulnerability in the HBook (h_book) extension 2.3.0 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6456 XF BID CONFIRM |
| matteoiammarrone -- s-cms | SQL injection vulnerability in admin/delete_page.php in S-Cms 1.1 Stable allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2009-03-10 | 7.5 | CVE-2009-0863 XF BID MILW0RM |
| matteoiammarrone -- s-cms | S-Cms 1.1 Stable allows remote attackers to bypass authentication and obtain administrative access via an OK value for the login cookie. | 2009-03-10 | 7.5 | CVE-2009-0864 XF BID MILW0RM |
| mediacommands | Multiple heap-based buffer overflows in Media Commands 1.0 allow remote attackers to execute arbitrary code or | 2009-03 | | CVE-2009-0885 XF |

| | | | | |
|---|---|---|---|---|
| mediacommands -- media_commands | cause a denial of service (application crash) via a long string in a (1) M3U, (2) M3l, (3) TXT, and (4) LRC playlist file. | 2009-03-12 | 9.3 | VUPEN MILW0RM SECUNIA OSVDB |
| mevin -- basic-php-events-lister | SQL injection vulnerability in event.php in Mevin Productions Basic PHP Events Lister 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2009-03-13 | 7.5 | CVE-2008-6464 BID |
| microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp | The graphics device interface (GDI) implementation in the kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate input received from user mode, which allows remote attackers to execute arbitrary code via a crafted (1) Windows Metafile (aka WMF) or (2) Enhanced Metafile (aka EMF) image file, aka "Windows Kernel Input Validation Vulnerability." | 2009-03-10 | 9.3 | CVE-2009-0081 MS |
| microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp | The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not properly validate handles, which allows local users to gain privileges via a crafted application that triggers unspecified "actions," aka "Windows Kernel Handle Validation Vulnerability." | 2009-03-10 | 7.2 | CVE-2009-0082 MS |
| microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 microsoft -- windows_vista microsoft -- windows_xp | The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 does not properly handle invalid pointers, which allows local users to gain privileges via an application that triggers use of a crafted pointer, aka "Windows Kernel Invalid Pointer Vulnerability." | 2009-03-10 | 7.2 | CVE-2009-0083 MS |
| microsoft -- windows_2000 microsoft -- windows_server_2003 | The Secure Channel (aka SChannel) authentication component in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008, when certificate authentication is used, does not properly validate the client's key | 2009-03 | | CVE-2009- |

| | | | | |
|---|---|---|---|---|
| microsoft -- windows_server_2008<br>microsoft -- windows_vista<br>microsoft -- windows_xp | not properly validate the client's key exchange data in Transport Layer Security (TLS) handshake messages, which allows remote attackers to spoof authentication by crafting a TLS packet based on knowledge of the certificate but not the private key, aka "SChannel Spoofing Vulnerability." | 2009-03-10 | 7.1 | 0085<br>MS |
| mirko_werner -- mw_random_objects | SQL injection vulnerability in the Simple Random Objects (mw_random_objects) extension 1.0.3 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6460<br>XF<br>BID<br>CONFIRM |
| mountaingrafix -- easylink | SQL injection vulnerability in detail.php in MountainGrafix easyLink 1.1.0 allows remote attackers to execute arbitrary SQL commands via the cat parameter in a show action. | 2009-03-13 | 7.5 | CVE-2008-6471<br>MILW0RM<br>SECUNIA |
| muskatli -- sofi_webgui | PHP remote file inclusion vulnerability in hu/modules/reg-new/modstart.php in Sofi WebGui 0.6.3 PRE and earlier allows remote attackers to execute arbitrary PHP code via a URL in the mod_dir parameter. | 2009-03-06 | 7.5 | CVE-2008-6402<br>XF<br>BID<br>MILW0RM |
| novastor -- novanet | Stack-based buffer overflow in the DtbClsLogin function in NovaStor NovaNET 12 allows remote attackers to (1) execute arbitrary code on Linux platforms via a long username field during backup domain authentication, related to libnnlindtb.so; or (2) cause a denial of service (daemon crash) on Windows platforms via a long username field during backup domain authentication, related to nnwindtb.dll. NOTE: some of these details are obtained from third party information. | 2009-03-09 | 10.0 | CVE-2009-0849<br>XF<br>BID<br>MISC<br>SECUNIA<br>OSVDB<br>OSVDB |
| oceandir -- oceandir | SQL injection vulnerability in show_vote.php in Oceandir 2.9 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2009-03-13 | 7.5 | CVE-2008-6452<br>BID<br>MILW0RM |
| | Buffer overflow in the server in | | | CVE-2008-3547<br>GENTOO |

| | | | | |
|---|---|---|---|---|
| openttd -- openttd | OpenTTD 0.6.1 and earlier allows remote authenticated users to cause a denial of service (persistent game disruption) or possibly execute arbitrary code via vectors involving many long names for "companies and clients." | 2009-03-10 | 9.0 | GENTOO<br>SECUNIA<br>MLIST<br>MLIST<br>MLIST<br>MLIST<br>CONFIRM<br>CONFIRM |
| phpkf -- phpkf | SQL injection vulnerability in forum_duzen.php in phpKF allows remote attackers to execute arbitrary SQL commands via the fno parameter. | 2009-03-09 | 7.5 | CVE-2008-6443<br>XF<br>MISC<br>BID |
| plaincart -- plaincart | SQL injection vulnerability in index.php in PlainCart 1.1.2 allows remote attackers to execute arbitrary SQL commands via the p parameter. | 2009-03-13 | 7.5 | CVE-2008-6469<br>BID<br>MILW0RM |
| roman_bogorodskiy -- nforum | Multiple SQL injection vulnerabilities in nForum 1.5 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to showtheme.php and the (2) user parameter to userinfo.php. | 2009-03-12 | 7.5 | CVE-2009-0882<br>BID<br>BUGTRAQ |
| torben_sorensen -- tinx/cms | SQL injection vulnerability in system/rss.php in TinX/cms 3.x before 3.5.1 allows remote attackers to execute arbitrary SQL commands via the id parameter. | 2009-03-09 | 7.5 | CVE-2009-0825<br>BID<br>CONFIRM |
| typo3 -- autobeuser | SQL injection vulnerability in the auto BE User Registration (autobeuser) extension 0.0.2 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6459<br>XF<br>BID<br>CONFIRM |
| walnutstreet -- cgswigmore | SQL injection vulnerability in the Swigmore institute (cgswigmore) extension before 0.1.2 for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | 2009-03-13 | 7.5 | CVE-2008-6457<br>CONFIRM |
| yourplace -- yourplace | Unspecified vulnerability in YourPlace before 1.0.1 has unknown impact and attack vectors, possibly related to improper authenticated and the ability to upload arbitrary PHP code. NOTE: | 2009-03-09 | 7.5 | CVE-2008-6445<br>CONFIRM |

| | | | | |
|---|---|---|---|---|
| | some of these details are obtained from third party information. | | | |

Back to top

| Medium Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary Vendor -- Product** | **Description** | **Published** | **CVSS Score** | **Source & Patch Info** |
| 6rbscript -- 6rbscript | Directory traversal vulnerability in section.php in 6rbScript 3.3, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the name parameter. | 2009-03-13 | 4.3 | CVE-2008-6453 MILW0RM |
| amunak -- blue_eye_cms | SQL injection vulnerability in Blue Eye CMS 1.0.0 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the BlueEyeCMS_login cookie parameter. | 2009-03-12 | 6.8 | CVE-2009-0883 XF BID MILW0RM |
| apache -- tomcat | Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat 4.1.0 through 4.1.39, 5.5.0 through 5.5.27, and 6.0.0 through 6.0.18 allows remote attackers to inject arbitrary web script or HTML via the time parameter, related to "invalid HTML." | 2009-03-09 | 4.3 | CVE-2009-0781 BUGTRAQ CONFIRM CONFIRM CONFIRM |
| apple -- itunes | Apple iTunes before 8.1 on Windows allows remote attackers to cause a denial of service (infinite loop) via a Digital Audio Access Protocol (DAAP) message with a crafted Content-Length header. | 2009-03-14 | 5.0 | CVE-2009-0016 CONFIRM APPLE |
| bitdefender -- internet_security | Cross-site scripting (XSS) vulnerability in BitDefender Internet Security 2009 allows user-assisted remote attackers to inject arbitrary web script or HTML via the filename of a | 2009-03-09 | 4.3 | CVE-2009-0850 VUPEN BUGTRAQ |

| | | | | |
|---|---|---|---|---|
| | virus-infected file, as demonstrated by a filename inside a (1) rar or (2) zip archive file. | | | BUGTRAQ<br>SECUNIA |
| centurysys -- xr-1100<br>centurysys -- xr-410<br>centurysys -- xr-410-l2<br>centurysys -- xr-440<br>centurysys -- xr-510<br>centurysys -- xr-540<br>centurysys -- xr-640<br>centurysys -- xr-640-l2<br>centurysys -- xr-730 | Cross-site request forgery (CSRF) vulnerability in multiple Century Systems routers including XR-410 before 1.6.9, XR-510 before 3.5.3, XR-440 before 1.7.8, and other XR series routers from XR-510 to XR-730 allows remote attackers to modify configuration as the administrator via unknown vectors. | 2009-03-09 | 4.0 | CVE-2008-6449<br>CONFIRM<br>JVNDB<br>JVN |
| cerberus -- cerberus_helpdesk<br>webgroupmedia -- cerberus_helpdesk | Cerberus Helpdesk before 4.0 (Build 600) allows remote attackers to obtain sensitive information via direct requests for "controllers ... that aren't standard helpdesk pages," possibly involving the (1) /display and (2) /kb URIs. | 2009-03-06 | 5.0 | CVE-2008-6440<br>BID<br>CONFIRM<br>SECUNIA |
| clansphere -- clansphere | Multiple unspecified vulnerabilities in ClanSphere before 2008.2.1 allow remote attackers to obtain sensitive information, and possibly have unknown other impact, via vectors related to "javascript insert" and the (1) mods/messages/getusers.php and (2) mods/abcode/listimg.php files. NOTE: some of these details are obtained from third party information. | 2009-03-13 | 5.0 | CVE-2008-6470<br>CONFIRM |
| d.j.bernstein -- djbdns | The response_addname function in response.c in Daniel J. Bernstein djbdns 1.05 and earlier does not constrain offsets in the required manner, which allows remote attackers, with control over a third-party subdomain served by tinydns and axfrdns, to trigger DNS responses containing arbitrary records via | 2009-03-09 | 5.8 | CVE-2009-0858<br>MISC |

| | | | | |
|---|---|---|---|---|
| | crafted zone data for this subdomain. | | | |
| dash -- dash | Untrusted search path vulnerability in dash 0.5.4, when used as a login shell, allows local users to execute arbitrary code via a Trojan horse .profile file in the current working directory. | 2009-03-11 | 6.9 | CVE-2009-0854<br>UBUNTU |
| denorastats -- phpdenora | Cross-site scripting (XSS) vulnerability in phpDenora before 1.2.3 allows remote attackers to inject arbitrary web script or HTML via an IRC channel name. NOTE: some of these details are obtained from third party information. | 2009-03-10 | 4.3 | CVE-2009-0861<br>BID<br>CONFIRM |
| edikon -- phpshop | Session fixation vulnerability in Edikon phpShop 0.8.1 allows remote attackers to hijack web sessions via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2009-03-13 | 6.8 | CVE-2008-6455<br>XF<br>BID<br>SECUNIA |
| filezilla -- filezilla_server | Buffer overflow in FileZilla Server before 0.9.31 allows remote attackers to cause a denial of service via unspecified vectors related to SSL/TLS packets. | 2009-03-12 | 5.0 | CVE-2009-0884<br>VUPEN<br>CONFIRM |
| foxit -- reader<br>foxit -- reader3.0 | Foxit Reader 2.3 before Build 3902 and 3.0 before Build 1506, including 1120 and 1301, does not require user confirmation before performing dangerous actions defined in a PDF file, which allows remote attackers to execute arbitrary programs and have unspecified other impact via a crafted file, as demonstrated by the "Open/Execute a file" action. | 2009-03-10 | 6.8 | CVE-2009-0836<br>CONFIRM |
| fujitsu -- enhanced_support_facility | The HRM-S service in Fujitsu Enhanced Support Facility 3.0 and 3.0.1 allows remote attackers to obtain (1) hardware and (2) | 2009-03-10 | 5.0 | CVE-2009-0867<br>XF<br>BID |

| | | | | |
|---|---|---|---|---|
| | software information via unspecified requests in a client connection. | 10 | | BID<br>CONFIRM<br>SECUNIA |
| fujitsu -- jasmine2000 | CRLF injection vulnerability in the WebLink template in Fujitsu Jasmine2000 Enterprise Edition allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. | 2009-03-10 | 6.8 | CVE-2009-0868<br>XF<br>BID<br>CONFIRM<br>SECUNIA |
| gnome -- glib | Multiple integer overflows in glib/gbase64.c in GLib before 2.20 allow context-dependent attackers to execute arbitrary code via a long string that is converted either (1) from or (2) to a base64 representation. | 2009-03-14 | 4.6 | CVE-2008-4316<br>BID<br>CONFIRM<br>MLIST<br>MISC |
| gnome -- evolution-data-server | The ntlm_challenge function in the NTLM SASL authentication mechanism in camel/camel-sasl-ntlm.c in Camel in Evolution Data Server (aka evolution-data-server) 2.24.5 and earlier, and 2.25.92 and earlier 2.25.x versions, does not validate whether a certain length value is consistent with the amount of data in a challenge packet, which allows remote mail servers to read information from the process memory of a client, or cause a denial of service (client crash), via an NTLM authentication type 2 packet with a length value that exceeds the amount of packet data. | 2009-03-14 | 5.8 | CVE-2009-0582<br>CONFIRM<br>XF<br>BID<br>SECTRACK<br>SECUNIA<br>MLIST |
| gnome -- evolution-data-server | Multiple integer overflows in Evolution Data Server (aka evolution-data-server) before 2.24.5 allow context-dependent attackers to execute arbitrary code via a long string that is converted to a base64 representation in (1) addressbook/libebook/e-vcard.c in evc or (2) camel/camel-mime- | 2009-03-14 | 4.6 | CVE-2009-0587<br>BID<br>MLIST<br>MISC<br>MISC |

| | | | | |
|---|---|---|---|---|
| | utils.c in libcamel. | | | |
| gstreamer -- gst-plugins-base | Integer overflow in gst-libs/gst/tag/gstvorbistag.c in vorbistag in gst-plugins-base (aka gstreamer-plugins-base) before 0.10.23 in GStreamer allows context-dependent attackers to execute arbitrary code via a long string that is converted from a base64 representation. | 2009-03-14 | 4.6 | CVE-2009-0586<br>BID<br>MLIST<br>MISC |
| hp -- systems_insight_manager | Unspecified vulnerability in WMI Mapper for HP Systems Insight Manager before 2.5.2.0 allows remote attackers to obtain sensitive information via unknown vectors. | 2009-03-11 | 5.0 | CVE-2009-0713<br>HP<br>HP |
| ibm -- websphere_application_server | Cross-site scripting (XSS) vulnerability in the administrative console in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.23 on z/OS allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | 2009-03-09 | 4.3 | CVE-2009-0855<br>VUPEN<br>BID<br>AIXAPAR<br>AIXAPAR<br>SECUNIA |
| ibm -- websphere_application_server | Multiple cross-site scripting (XSS) vulnerabilities in sample applications in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.23 on z/OS allow remote attackers to inject arbitrary web script or HTML via unspecified vectors. | 2009-03-09 | 4.3 | CVE-2009-0856<br>AIXAPAR |
| ibm -- director | The CIM server in IBM Director before 5.20.3 Service Update 2 on Windows allows remote attackers to cause a denial of service (daemon crash) via a long consumer name, as demonstrated by an M-POST request to a long /CIMListener/ URI. | 2009-03-12 | 5.0 | CVE-2009-0879<br>MISC<br>VUPEN |
| | Directory traversal vulnerability in the CIM server in IBM Director before 5.20.3 Service | | | CVE-2009 |

| | | | | |
|---|---|---|---|---|
| ibm -- director | Update 2 on Windows allows remote attackers to load and execute arbitrary local DLL code via a .. (dot dot) in a /CIMListener/ URI in an M-POST request. | 2009-03-12 | 6.8 | CVE-2009-0880<br>MISC<br>VUPEN |
| joe_shaw -- libsoup | Integer overflow in the soup_base64_encode function in soup-misc.c in libsoup 2.x.x before 2.2.x, and 2.x before 2.24, allows context-dependent attackers to execute arbitrary code via a long string that is converted to a base64 representation. | 2009-03-14 | 4.6 | CVE-2009-0585<br>BID<br>MLIST<br>MISC |
| kernel -- linux | The shm_get_stat function in ipc/shm.c in the shm subsystem in the Linux kernel before 2.6.28.5, when CONFIG_SHMEM is disabled, misinterprets the data type of an inode, which allows local users to cause a denial of service (system hang) via an SHM_INFO shmctl call, as demonstrated by running the ipcs program. | 2009-03-09 | 4.7 | CVE-2009-0859<br>BID<br>CONFIRM<br>MLIST<br>MLIST<br>MLIST<br>MLIST<br>CONFIRM<br>CONFIRM |
| kernel -- linux-pam | Integer signedness error in the _pam_StrTok function in libpam/pam_misc.c in Linux-PAM (aka pam) 1.0.3 and earlier, when a configuration file contains non-ASCII usernames, might allow remote attackers to cause a denial of service, and might allow remote authenticated users to obtain login access with a different user's non-ASCII username, via a login attempt. | 2009-03-12 | 6.6 | CVE-2009-0887<br>BID<br>CONFIRM |
| lukas_waldauf -- phpfreeforum | Multiple cross-site scripting (XSS) vulnerabilities in PHPFreeForum 1.0 RC2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) message parameter to error.php, and the | 2009-03-06 | 4.3 | CVE-2008-6437<br>XF<br>BID<br>BUGTRAQ<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| | (2) nickname and (3) randomid parameters to part/menu.php. | | | SECUNIA |
| mahara -- mahara | Multiple cross-site scripting (XSS) vulnerabilities in Mahara 1.0 before 1.0.10 and 1.1 before 1.1.2 allow remote attackers to inject arbitrary web script or HTML via a (1) profile and (2) blog, a different vulnerability than CVE-2009-0487. | 2009-03-11 | 4.3 | CVE-2009-0660<br>BID |
| microsoft -- interix<br>openbsd -- openbsd | Integer overflow in the fts_build function in fts.c in libc in (1) OpenBSD 4.4 and earlier and (2) Microsoft Interix 6.0 build 10.0.6030.0 allows context-dependent attackers to cause a denial of service (application crash) via a deep directory tree, related to the fts_level structure member, as demonstrated by (a) du, (b) rm, (c) chmod, and (d) chgrp on OpenBSD; and (e) SearchIndexer.exe on Vista Enterprise. | 2009-03-09 | 4.9 | CVE-2009-0537<br>BID<br>BUGTRAQ<br>CONFIRM<br>CONFIRM<br>MILW0RM<br>SREASONRES |
| microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_server_2008 | The WINS server in Microsoft Windows 2000 SP4 and Server 2003 SP1 and SP2 does not restrict registration of the (1) "wpad" and (2) "isatap" NetBIOS names, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) and Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) features, and conduct man-in-the-middle attacks by spoofing a proxy server or ISATAP route, by registering one of these names in the WINS database, aka "WPAD WINS Server Registration Vulnerability," a related issue to CVE-2007-1692. | 2009-03-11 | 4.0 | CVE-2009-0094<br>MS |
| | The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in | | | |

| | | | | |
|---|---|---|---|---|
| microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_server_2008 | Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not reuse cached DNS responses in all applicable situations, which makes it easier for remote attackers to predict transaction IDs and poison caches by simultaneously sending crafted DNS queries and responses, aka "DNS Server Query Validation Vulnerability." | 2009-03-11 | 5.8 | CVE-2009-0233<br>MS |
| microsoft -- windows_2000<br>microsoft -- windows_server_2003<br>microsoft -- windows_server_2008 | The DNS Resolver Cache Service (aka DNSCache) in Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008 does not properly cache crafted DNS responses, which makes it easier for remote attackers to predict transaction IDs and poison caches by sending many crafted DNS queries that trigger "unnecessary lookups," aka "DNS Server Response Validation Vulnerability." | 2009-03-11 | 6.4 | CVE-2009-0234<br>MS |
| netcordia -- netmri | Cross-site scripting (XSS) vulnerability in the web user interface in the login application in NetMRI 3.0.1 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to error pages. | 2009-03-10 | 4.3 | CVE-2009-0860<br>BID<br>BUGTRAQ<br>SECUNIA<br>CONFIRM |
| oneorzero -- oneorzero_helpdesk | Directory traversal vulnerability in login.php in OneOrZero Helpdesk 1.6.5.7 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the default_language parameter. | 2009-03-12 | 5.0 | CVE-2009-0886<br>XF<br>BID<br>MILW0RM<br>MILW0RM |
| opensuse -- opensuse | Untrusted search path vulnerability in GTK2 in OpenSUSE 11.0 and 11.1 allows local users to execute arbitrary | 2009-03-11 | 4.4 | CVE-2009-0848 |

| | | | | |
|---|---|---|---|---|
| | code via a Trojan horse GTK module in an unspecified "relative search path." | 11 | | SUSE |
| parallels -- h-sphere | Multiple cross-site scripting (XSS) vulnerabilities in login.php in webshell4 in Parallels H-Sphere 3.0.0 P9 and 3.1 P1 allow remote attackers to inject arbitrary web script or HTML via the (1) err, (2) errorcode, and (3) login parameters. | 2009-03-13 | 4.3 | CVE-2008-6465<br>XF<br>XF<br>MISC<br>BID<br>SECUNIA |
| phnews -- phnews | pHNews Alpha 1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for extra/genbackup.php. | 2009-03-10 | 5.0 | CVE-2009-0866<br>XF<br>MILW0RM |
| quiksoft -- easymail_mailstore | Buffer overflow in emmailstore.dll 6.5.0.3 in the QuikSoft EasyMail MailStore ActiveX control allows remote attackers to execute arbitrary code via a long first argument to the CreateStore method. | 2009-03-09 | 6.8 | CVE-2008-6447<br>XF<br>BID<br>MILW0RM |
| redhat -- jboss_enterprise_application_platform | The request handler in JBossWS in JBoss Enterprise Application Platform (aka JBoss EAP or JBEAP) 4.2 before 4.2.0.CP06 and 4.3 before 4.3.0.CP04 does not properly validate the resource path during a request for a WSDL file with a custom web-service endpoint, which allows remote attackers to read arbitrary XML files via a crafted request. | 2009-03-09 | 5.0 | CVE-2009-0027<br>REDHAT<br>REDHAT<br>REDHAT |
| sina -- dloader | Insecure method vulnerability in Sina Inc. DLoader Class ActiveX Control allows remote attackers to overwrite arbitrary files via a URL in the first parameter to the DonwloadAndInstall method. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | 2009-03-09 | 5.8 | CVE-2008-6442<br>XF<br>BID<br>MISC |

| | | | | |
|---|---|---|---|---|
| skyarc -- mtcms_wysiwyg_editor | Cross-site scripting (XSS) vulnerability in install.cgi in SKYARC System MTCMS WYSIWYG Editor allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | 2009-03-09 | 4.3 | CVE-2008-6448 CONFIRM JVNDB JVN |
| stewart_howe -- celerbb | Multiple SQL injection vulnerabilities in CelerBB 0.0.2, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the id parameter to (1) viewforum.php and (2) viewtopic.php. | 2009-03-09 | 6.8 | CVE-2009-0851 BID BUGTRAQ MILW0RM |
| stewart_howe -- celerbb | showme.php in CelerBB 0.0.2 allows remote attackers to obtain "reserved information" via the user parameter. | 2009-03-09 | 5.0 | CVE-2009-0852 BID BUGTRAQ MILW0RM |
| stewart_howe -- celerbb | login.php in CelerBB 0.0.2, when magic_quotes_gpc is disabled, allows remote attackers to bypass authentication and obtain administrative access via special characters in the Username parameter, as demonstrated by an admin'# parameter value. | 2009-03-09 | 6.8 | CVE-2009-0853 BID BUGTRAQ MILW0RM |
| sun -- opensolaris<br>sun -- solaris | The crypto pseudo device driver in Sun Solaris 10, and OpenSolaris snv_88 through snv_102, does not properly free memory, which allows local users to cause a denial of service (panic) via unspecified vectors, related to the vmem_hash_delete function. | 2009-03-06 | 4.9 | CVE-2009-0838 SUNALERT CONFIRM |
| sun -- management_center | Cross-site scripting (XSS) vulnerability in /prm/reports in the Performance Reporting Module (PRM) for Sun Management Center (SunMC) 3.6.1 and 4.0 allows remote attackers to inject arbitrary web script or HTML via the msg | 2009-03-09 | 4.3 | CVE-2009-0857 BID SUNALERT CONFIRM |

| | | | | |
|---|---|---|---|---|
| | parameter. NOTE: this can be leveraged for access to the SunMC Web Console. | | | |
| sun -- opensolaris<br>sun -- solaris | The NFSv4 Server module in the kernel in Sun Solaris 10, and OpenSolaris before snv_111, allow local users to cause a denial of service (infinite loop and system hang) by accessing an hsfs filesystem that is shared through NFSv4, related to the rfs4_op_readdir function. | 2009-03-10 | 4.9 | CVE-2009-0870<br>BID<br>SUNALERT<br>CONFIRM |
| sun -- opensolaris<br>sun -- solaris | The NFS server in Sun Solaris 10, and OpenSolaris before snv_111, does not properly implement the AUTH_NONE (aka sec=none) security mode in combination with other security modes, which allows remote attackers to bypass intended access restrictions and read or modify files, as demonstrated by a combination of the AUTH_NONE and AUTH_SYS security modes. | 2009-03-11 | 6.8 | CVE-2009-0872<br>SUNALERT<br>CONFIRM |
| sun -- opensolaris<br>sun -- solaris | The NFS daemon (aka nfsd) in Sun Solaris 10 and OpenSolaris before snv_106, when NFSv3 is used, does not properly implement combinations of security modes, which allows remote attackers to bypass intended access restrictions and read or modify files, as demonstrated by a combination of the sec=sys and sec=krb5 security modes, related to modes that "override each other." | 2009-03-11 | 6.8 | CVE-2009-0873<br>SUNALERT<br>CONFIRM |
| sun -- opensolaris | Multiple unspecified vulnerabilities in the Doors subsystem in the kernel in Sun Solaris 8 through 10, and OpenSolaris before snv_94, allow local users to cause a denial of service (process hang), or possibly bypass file | 2009-03- | 4.9 | CVE-2009-0874 |

| | | | | |
|---|---|---|---|---|
| sun -- solaris | or possibly bypass file permissions or gain kernel-context privileges, via vectors including ones related to (1) an argument handling deadlock in a door server and (2) watchpoint problems in the door_call function. | 12 | 4.9 | SUNALERT CONFIRM |
| sun -- opensolaris<br>sun -- solaris | Race condition in the Doors subsystem in the kernel in Sun Solaris 8 through 10, and OpenSolaris before snv_94, allows local users to cause a denial of service (process hang), or possibly bypass file permissions or gain kernel-context privileges, via vectors involving the time at which control is transferred from a caller to a door server. | 2009-03-12 | 6.9 | CVE-2009-0875 SUNALERT CONFIRM |
| sun -- xvm_virtualbox | Unspecified vulnerability in Sun xVM VirtualBox 2.0.0, 2.0.2, 2.0.4, 2.0.6r39760, 2.1.0, 2.1.2, and 2.1.4r42893 on Linux allows local users to gain privileges via unknown vectors related to "certain packages." | 2009-03-12 | 6.9 | CVE-2009-0876 SUNALERT |
| sun -- java_system_communications_express | Multiple cross-site scripting (XSS) vulnerabilities in Sun Java System Communications Express allow remote attackers to inject arbitrary web script or HTML via the (1) Full Name or (2) Subject field. | 2009-03-12 | 4.3 | CVE-2009-0877 BID BUGTRAQ MISC |
| tangocms -- tangocms | Cross-site scripting (XSS) vulnerability in the hook_cntrlr_error_output function in modules/page/hooks/listeners.php in the admincp component in TangoCMS 2.2.x (aka Eagle) before 2.2.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: some of these details are obtained from third | 2009-03-10 | 4.3 | CVE-2009-0862 CONFIRM CONFIRM |

| | | | | |
|---|---|---|---|---|
| | party information. | | | |
| under_construction_baby -- pc2m | Cross-site scripting (XSS) vulnerability in Under Construction, Baby (UCB) PC2M 0.9.22.4 and earlier allows remote attackers to inject arbitrary web script or HTML via unknown vectors. | 2009-03-09 | 4.3 | CVE-2008-6450 CONFIRM JVNDB JVN |
| wesnoth -- wesnoth | The uncompress_buffer function in src/server/simple_wml.cpp in Wesnoth before r33069 allows remote attackers to cause a denial of service via a large compressed WML document. | 2009-03-12 | 4.3 | CVE-2009-0366 CONFIRM BID DEBIAN CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM |
| wesnoth -- wesnoth | The read_game_map function in src/terrain_translation.cpp in Wesnoth before r32987 allows remote attackers to cause a denial of service (memory consumption and daemon hang) via a map with a large (1) width or (2) height. | 2009-03-12 | 5.0 | CVE-2009-0878 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM |
| wireshark -- wireshark | The WLCCP dissector in Wireshark 0.99.7 through 1.0.4 allows remote attackers to cause a denial of service (infinite loop) via unspecified vectors. | 2009-03-14 | 4.3 | CVE-2008-6472 CONFIRM |
| xerox -- workcentre | Cross-site scripting (XSS) vulnerability in the Web Server in Xerox WorkCentre 7132, 7228, 7235, and 7245 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | 2009-03-06 | 4.3 | CVE-2008-6436 CONFIRM VUPEN |

Back to top

| Low Vulnerabilities | | | | |
|---|---|---|---|---|
| **Primary** | **Description** | **Published** | **CVSS** | **Source &** |

| Vendor -- Product | Description | Published | Score | Patch Info |
|---|---|---|---|---|
| digium -- asterisk | The SIP channel driver in Asterisk Open Source 1.4.22, 1.4.23, and 1.4.23.1; 1.6.0 before 1.6.0.6; 1.6.1 before 1.6.1.0-rc2; and Asterisk Business Edition C.2.3, with the pedantic option enabled, allows remote authenticated users to cause a denial of service (crash) via a SIP INVITE request without any headers, which triggers a NULL pointer dereference in the (1) sip_uri_headers_cmp and (2) sip_uri_params_cmp functions. | 2009-03-11 | 3.5 | CVE-2009-0871 BID CONFIRM |
| microsoft -- windows_2000 microsoft -- windows_server_2003 microsoft -- windows_server_2008 | Windows DNS Server in Microsoft Windows 2000 SP4, Server 2003 SP1 and SP2, and Server 2008, when dynamic updates are enabled, does not restrict registration of the "wpad" hostname, which allows remote authenticated users to hijack the Web Proxy Auto-Discovery (WPAD) feature, and conduct man-in-the-middle attacks by spoofing a proxy server, via a Dynamic Update request for this hostname, aka "DNS Server Vulnerability in WPAD Registration Vulnerability," a related issue to CVE-2007-1692. | 2009-03-11 | 3.5 | CVE-2009-0093 MS |
| slysoft -- anydvd slysoft -- clonecd slysoft -- clonedvd slysoft -- virtualclonedrive | Elaborate Bytes ElbyCDIO.sys 6.0.2.0 and earlier, as distributed in SlySoft AnyDVD before 6.5.2.6, Virtual CloneDrive 5.4.2.3 and earlier, CloneDVD 2.9.2.0 and earlier, and CloneCD 5.3.1.3 and earlier, uses the METHOD_NEITHER communication method for IOCTLs and does not properly validate a buffer associated with the Irp object, which allows local users to cause a denial of service (system crash) via a crafted IOCTL call. | 2009-03-14 | 2.1 | CVE-2009-0824 BID BUGTRAQ MISC |

Back to top