

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.

<b>High Vulnerabilities</b>				
<b>Primary Vendor -- Product</b>	<b>Description</b>	<b>Published</b>	<b>CVSS Score</b>	<b>Source &amp; Patch Info</b>
123flashchat -- echat_plugin	SQL injection vulnerability in e107chat.php in the eChat plugin 4.2 for e107, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the nick parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2008-6069</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a>
a4desk -- a4desk_flash_event_calendar	SQL injection vulnerability in A4Desk PHP Event Calendar allows remote attackers to execute arbitrary SQL commands via the eventid parameter to admin/index.php.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2008-6104</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
apple -- mac_os_x apple -- mac_os_x_server	Certificate Assistant in Apple Mac OS X 10.5.6 allows local users to overwrite arbitrary files via unknown vectors related to an "insecure file operation" on a temporary file.	2009-02-12	<a href="#">7.2</a>	<a href="#">CVE-2009-0011</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in CoreText in Apple Mac OS X 10.5.6 allows remote attackers to execute arbitrary code via a crafted Unicode string.	2009-02-12	<a href="#">10.0</a>	<a href="#">CVE-2009-0012</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	csregprinter in the Printing component in Apple Mac OS X 10.4.11 and 10.5.6 does not properly handle error conditions, which allows local users to execute arbitrary code via unknown vectors that trigger a heap-based buffer overflow.	2009-02-12	<a href="#">7.2</a>	<a href="#">CVE-2009-0017</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	The Remote Apple Events server in Apple Mac OS X 10.4.11 and 10.5.6 does not properly initialize a buffer, which allows remote attackers to read portions of memory.	2009-02-12	<a href="#">7.8</a>	<a href="#">CVE-2009-0018</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	Remote Apple Events in Apple Mac OS X 10.4.11 and 10.5.6 allows remote attackers to cause a denial of service (application termination) or obtain sensitive information via unspecified vectors that	2009-02-12	<a href="#">7.5</a>	<a href="#">CVE-2009-0019</a> <a href="#">APPLE</a>

	trigger an out-of-bounds memory access.			
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in CarbonCore in Apple Mac OS X 10.4.11 and 10.5.6 allows remote attackers to cause a denial of service (application termination) and execute arbitrary code via a crafted resource fork that triggers memory corruption.	2009-02-12	7.8	<a href="#">CVE-2009-0020</a> <a href="#">APPLE</a>
apple -- safari	Multiple unspecified vulnerabilities in Safari RSS in Apple Mac OS X 10.4.11 and 10.5.6, and Windows XP and Vista, allow remote attackers to execute arbitrary JavaScript in the local security zone via a crafted feed: URL, related to "input validation issues."	2009-02-12	10.0	<a href="#">CVE-2009-0137</a> <a href="#">APPLE</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	servermgrd (Server Manager) in Apple Mac OS X 10.5.6 does not properly validate authentication credentials, which allows remote attackers to modify the system configuration.	2009-02-12	10.0	<a href="#">CVE-2009-0138</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	Integer overflow in the SMB component in Apple Mac OS X 10.5.6 allows remote SMB servers to cause a denial of service (system shutdown) or execute arbitrary code via a crafted SMB file system that triggers a heap-based buffer overflow.	2009-02-12	9.3	<a href="#">CVE-2009-0139</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in the SMB component in Apple Mac OS X 10.4.11 and 10.5.6 allows remote SMB servers to cause a denial of service (memory exhaustion and system shutdown) via a crafted file system name.	2009-02-12	9.3	<a href="#">CVE-2009-0140</a> <a href="#">APPLE</a>
areva -- e-terrahabitat	Unspecified vulnerability in the WebFGServer application in AREVA e-terrahabitat 5.7 and earlier allows remote attackers to cause a denial of service (system crash) via unknown vectors, aka PD32018.	2009-02-08	7.8	<a href="#">CVE-2009-0211</a> <a href="#">CERT-VN</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
aspindir -- mydesign_sayac	Multiple SQL injection vulnerabilities in default.asp in MyDesign Sayac 2.0 allow remote attackers to execute arbitrary SQL commands via (1) the user parameter (aka UserName field) or (2) the pass parameter (aka Pass field) to (a) admin/admin.asp or (b) the default URI under admin/. NOTE: some of these details are obtained from third party information.	2009-02-10	7.5	<a href="#">CVE-2009-0447</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
audacity -- audacity	Stack-based buffer overflow in the String_parse::get_nonspace_quoted function in lib-src/allegro/strparse.cpp in Audacity 1.2.6 and other versions before 1.3.6 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a .gro file containing a long string.	2009-02-09	9.3	<a href="#">CVE-2009-0490</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
blazevideo -- hdtv_player	Stack-based buffer overflow in BlazeVideo HDTV Player 3.5 and earlier allows remote attackers to execute arbitrary code via a long string in a playlist (aka .plf) file.	2009-02-10	9.3	<a href="#">CVE-2009-0450</a> <a href="#">BID</a> <a href="#">MILWORM</a>

businessspace -- businessspace	SQL injection vulnerability in the classified page (classified.php) in BusinessSpace 1.2 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0516</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
clicktech -- clickcart	Multiple SQL injection vulnerabilities in customer_login_check.asp in ClickTech ClickCart 6.0 allow remote attackers to execute arbitrary SQL commands via (1) the txtEmail parameter (aka E-MAIL field) or (2) the txtPassword parameter (aka password field) to customer_login.asp. NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0462</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
dmxready -- online_notebook_manager	Multiple SQL injection vulnerabilities in DMXReady Online Notebook Manager 1.1 allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password field. NOTE: some third parties report inability to verify this issue.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0454</a> <a href="#">BID</a> <a href="#">MILWORM</a>
dreampics -- gallery_builder	SQL injection vulnerability in index.php in Dreampics Gallery Builder allows remote attackers to execute arbitrary SQL commands via the exhibition_id parameter in a gallery.viewPhotos action.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0445</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
elecard -- elecard_mpeg_player	Stack-based buffer overflow in Elecard MPEG Player 5.5 build 15884.081218 allows remote attackers to execute arbitrary code via a M3U file containing a long URL.	2009-02-09	<a href="#">9.3</a>	<a href="#">CVE-2009-0491</a> <a href="#">MILWORM</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
elecard -- elecard_avc_hd_player	Stack-based buffer overflow in Elecard AVC HD PLAYER 5.5.90116 allows remote attackers to execute arbitrary code via an M3U file containing a long string in a URL.	2009-02-10	<a href="#">9.3</a>	<a href="#">CVE-2009-0443</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
electrictoad -- snippetmaster_webpage_editor	Multiple PHP remote file inclusion vulnerabilities in SnippetMaster 2.2.2, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) _SESSION[SCRIPT_PATH] parameter to includes/vars.inc.php and the (2) g_pcldr_lib_dir parameter to includes/tar_lib/pcldr.lib.php.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2009-0530</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
extrosoft -- com_thyme	SQL injection vulnerability in the EXtrovert Software Thyme (com_thyme) 1.0 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the event parameter to index.php.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6116</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a>
extrosoft -- thyme	Directory traversal vulnerability in export.php in Thyme 1.3 and earlier, when register_globals is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the export_to parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2009-0535</a> <a href="#">MILWORM</a>
	SQL injection vulnerability in click.php in Adult			<a href="#">CVE-2008-6101</a>

ezonescripts -- adult_banner_exchange_website	Banner Exchange Website allows remote attackers to execute arbitrary SQL commands via the targetid parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">XF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
ezonescripts -- link_trader_script	SQL injection vulnerability in ratelink.php in Link Trader Script allows remote attackers to execute arbitrary SQL commands via the lnkid parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2008-6102</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
flexcms -- flexcms	SQL injection vulnerability in FlexCMS allows remote attackers to execute arbitrary SQL commands via the catId parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2009-0534</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a>
futomis_cgi_cafe -- fulltext_search_cgi	Unspecified vulnerability in futomi's CGI Cafe Fulltext search CGI 1.1.2 allows remote attackers to gain administrative privileges via unknown vectors.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0469</a> <a href="#">CONFIRM</a> <a href="#">JVNDDB</a> <a href="#">JVN</a>
ge_fanuc -- ifix	GE Fanuc iFIX 5.0 and earlier relies on client-side authentication involving a weakly encrypted local password file, which allows remote attackers to bypass intended access restrictions and start privileged server login sessions by recovering a password or by using a modified program module.	2009-02-13	<a href="#">10.0</a>	<a href="#">CVE-2009-0216</a> <a href="#">CERT-VN</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">CONFIRM</a>
goople_cms -- goople_cms	win/content/upload.php in Google CMS 1.7 allows remote attackers to bypass authentication and gain administrative access by setting the loggedin cookie to 1.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6118</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
goople_cms -- google_cms	Static code injection vulnerability in gooplecms/admin/account/action/editpass.php in Google CMS 1.7 allows remote attackers to inject arbitrary PHP code into admin/userandpass.php via the (1) username and (2) password parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6119</a> <a href="#">SECUNIA</a>
graphicsmagick -- graphicsmagick	Multiple heap-based buffer underflows in the ReadPALMImage function in coders/palm.c in GraphicsMagick before 1.2.3 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted PALM image, a different vulnerability than CVE-2007-0770. NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">9.3</a>	<a href="#">CVE-2008-6070</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a>
graphicsmagick -- graphicsmagick	Heap-based buffer overflow in the DecodeImage function in coders/pict.c in GraphicsMagick before 1.1.14, and 1.2.x before 1.2.3, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted PICT image. NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">10.0</a>	<a href="#">CVE-2008-6071</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a>

[CVE 2009](#)

groonesworld -- glinks	PHP remote file inclusion vulnerability in includes/header.php in Groone GLinks 2.1 allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0463</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
ibm -- websphere_application_server	CRLF injection vulnerability in the WebContainer component in IBM WebSphere Application Server (WAS) 5.1.1.19 and earlier 5.1.x versions allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors.	2009-02-10	<a href="#">10.0</a>	<a href="#">CVE-2008-4283</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">AIXAPAR</a>
ibm -- websphere_application_server	The (1) mod_ibm_ssl and (2) mod_cgid modules in IBM HTTP Server 6.0.x before 6.0.2.31 and 6.1.x before 6.1.0.19, as used in WebSphere Application Server (WAS), set incorrect permissions for AF_UNIX sockets, which has unknown impact and local attack vectors.	2009-02-10	<a href="#">10.0</a>	<a href="#">CVE-2009-0436</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
it!cms -- it!cms	SQL injection vulnerability in login.php in IT!CMS 2.1a and earlier allows remote attackers to execute arbitrary SQL commands via the Username.	2009-02-09	<a href="#">7.5</a>	<a href="#">CVE-2009-0493</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a>
it747 -- realtor_747	PHP remote file inclusion vulnerability in include/define.php in REALTOR 747 4.11 allows remote attackers to execute arbitrary PHP code via a URL in the INC_DIR parameter.	2009-02-09	<a href="#">7.5</a>	<a href="#">CVE-2009-0495</a> <a href="#">BID</a> <a href="#">MILWORM</a>
kaspersky_lab -- kaspersky_antivirus	Buffer overflow in klim5.sys in Kaspersky Anti-Virus for Workstations 6.0 and Anti-Virus 2008 allows local users to gain privileges via an IOCTL 0x80052110 call.	2009-02-10	<a href="#">7.2</a>	<a href="#">CVE-2009-0449</a> <a href="#">MISC</a> <a href="#">SECTRACK</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
magtrb -- aja_portal	Multiple directory traversal vulnerabilities in AJA Portal 1.2 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the currentlang parameter to admin/case.php in the (1) Contact_Plus and (2) Reviews modules, and (3) the module_name parameter to admin/includes/FANCYNLOptions.php in the Fancy_NewsLetter module.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0457</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a> <a href="#">OSVDB</a>
microsoft -- internet_explorer	Microsoft Internet Explorer 7 does not properly handle errors during attempted access to deleted objects, which allows remote attackers to execute arbitrary code via a crafted HTML document, related to CFunctionPointer and the appending of document objects, aka "Uninitialized Memory Corruption Vulnerability."	2009-02-10	<a href="#">8.5</a>	<a href="#">CVE-2009-0075</a> <a href="#">MS</a>
microsoft -- internet_explorer	Microsoft Internet Explorer 7, when XHTML strict mode is used, allows remote attackers to execute arbitrary code via the zoom style directive in conjunction with unspecified other directives in a malformed Cascading Style Sheets (CSS) stylesheet	2009-02-10	<a href="#">9.3</a>	<a href="#">CVE-2009-0076</a> <a href="#">MS</a>

	in a crafted HTML document, aka "CSS Memory Corruption Vulnerability."			
microsoft -- visio	Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 does not properly validate object data in Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Memory Validation Vulnerability."	2009-02-10	9.3	<a href="#">CVE-2009-0095</a> <a href="#">MS</a>
microsoft -- visio	Microsoft Office Visio 2002 SP2, 2003 SP3, and 2007 SP1 does not properly perform memory copy operations for object data, which allows remote attackers to execute arbitrary code via a crafted Visio document, aka "Memory Corruption Vulnerability."	2009-02-10	9.3	<a href="#">CVE-2009-0096</a> <a href="#">MS</a>
microsoft -- visio	Microsoft Office Visio 2002 SP2 and 2003 SP3 does not properly validate memory allocation for Visio files, which allows remote attackers to execute arbitrary code via a crafted file, aka "Memory Corruption Vulnerability."	2009-02-10	9.3	<a href="#">CVE-2009-0097</a> <a href="#">MS</a>
microsoft -- exchange_server	Microsoft Exchange 2000 Server SP3, Exchange Server 2003 SP2, and Exchange Server 2007 SP1 do not properly interpret Transport Neutral Encapsulation (TNEF) properties, which allows remote attackers to execute arbitrary code via a crafted TNEF message, aka "Memory Corruption Vulnerability."	2009-02-10	9.3	<a href="#">CVE-2009-0098</a> <a href="#">MS</a>
mivaco -- com_portfol	SQL injection vulnerability in the Portfol (com_portfol) 1.2 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the vcatid parameter in a viewcategory action to index.php.	2009-02-09	7.5	<a href="#">CVE-2009-0494</a> <a href="#">BID</a> <a href="#">MILWORM</a>
moodle -- moodle	SQL injection vulnerability in the hotpot_delete_selected_attempts function in report.php in the HotPot module in Moodle 1.6 before 1.6.7, 1.7 before 1.7.5, 1.8 before 1.8.6, and 1.9 before 1.9.2 allows remote attackers to execute arbitrary SQL commands via a crafted selected attempt.	2009-02-12	7.5	<a href="#">CVE-2008-6124</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Bugzilla 3.2.1, 3.0.7, and 3.3.2, when running under mod_perl, calls the srand function at startup time, which causes Apache children to have the same seed and produce insufficiently random numbers for random tokens, which allows remote attackers to bypass cross-site request forgery (CSRF) protection mechanisms and conduct unauthorized activities as other users.	2009-02-09	7.5	<a href="#">CVE-2009-0486</a> <a href="#">CONFIRM</a>
multimediasoft -- audio_dj_studio_for_.net multimediasoft -- audio_sound_editer_for_.net multimediasoft -- audio_sound_recorder_for_.net multimediasoft -- audio_sound_studio_for_.net multimediasoft -- audio_sound_suite_for_.net	Stack-based buffer overflow in MultiMedia Soft AdjMmsEng.dll 7.11.1.0 and 7.11.2.7, as distributed in multiple MultiMedia Soft audio components for .NET, allows remote attackers to execute arbitrary code via a long string in a playlist (.pls) file, as originally reported for Euphonics Audio Player 1.0. NOTE: some of these details are obtained from third party information.	2009-02-08	9.3	<a href="#">CVE-2009-0476</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a> <a href="#">MILWORM</a> <a href="#">MILWORM</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">SECUNIA</a>

mytipper -- zogo_shop	SQL injection vulnerability in product_details.php in the Mytipper Zogo_shop 1.15.4 plugin for e107 allows remote attackers to execute arbitrary SQL commands via the product parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6114</a> <a href="#">BID</a> <a href="#">MILWORM</a>
netart_media -- vlog_system	SQL injection vulnerability in blog.php in NetArt Media Vlog System 1.1 allows remote attackers to execute arbitrary SQL commands via the note parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6111</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
netgear -- wgr614	The web management interface in Netgear WGR614v9 allows remote attackers to cause a denial of service (crash) via a request that contains a question mark ("?").	2009-02-11	<a href="#">7.8</a>	<a href="#">CVE-2008-6122</a> <a href="#">BID</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a> <a href="#">FULLDISC</a>
newsgator -- feeddemon	Stack-based buffer overflow in NewsGator FeedDemon 2.7 and earlier allows user-assisted remote attackers to execute arbitrary code via a long text attribute in an outline element in a .opml file.	2009-02-12	<a href="#">9.3</a>	<a href="#">CVE-2009-0546</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a> <a href="#">MILWORM</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
ontarioabandonedplaces -- a_better_member-based_asp_photo_gallery	SQL injection vulnerability in gallery/view.asp in A Better Member-Based ASP Photo Gallery before 1.2 allows remote attackers to execute arbitrary SQL commands via the entry parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2009-0531</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
phpscripts -- ranking-script	phpscripts Ranking Script allows remote attackers to bypass authentication and gain administrative access by sending an admin=ja cookie.	2009-02-09	<a href="#">7.5</a>	<a href="#">CVE-2008-6092</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
phpslash -- phpslash	Eval injection vulnerability in index.php in phpSlash 0.8.1.1 and earlier allows remote attackers to execute arbitrary PHP code via the fields parameter, which is supplied to an eval function call within the generic function in include/class/tz_env.class. NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">10.0</a>	<a href="#">CVE-2009-0517</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
pilotgroup -- pg_job_site_pro	SQL injection vulnerability in homepage.php in PG Job Site Pro allows remote attackers to execute arbitrary SQL commands via the poll_view_id parameter in a results action.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6117</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
proftpd_project -- proftpd	SQL injection vulnerability in ProFTPD Server 1.3.1 through 1.3.2rc2 allows remote attackers to execute arbitrary SQL commands via a "%" (percent) character in the username, which	2009-02-12	<a href="#">7.5</a>	<a href="#">CVE-2009-0542</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">BUGTRAQ</a> <a href="#">MFTIST</a>

	introduces a ' (single quote) character during variable substitution by mod_sql.			<a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MILWORM</a> <a href="#">CONFIRM</a>
mozilla -- hosting_index	SQL injection vulnerability in directory.php in Mozilla Hosting Index allows remote attackers to execute arbitrary SQL commands via the id parameter in a deadlink action, a different vector than CVE-2008-2083.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6115</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
pycrypto -- arc2	Buffer overflow in the PyCrypto ARC2 module 2.0.1 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a large ARC2 key length.	2009-02-12	<a href="#">10.0</a>	<a href="#">CVE-2009-0544</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
realnetworks -- realplayer	A DLL file in RealNetworks RealPlayer 11 allows remote attackers to execute arbitrary code via a crafted Internet Video Recording (IVR) file with a filename length field containing a large integer, which triggers overwrite of an arbitrary memory location with a 0x00 byte value, related to use of RealPlayer through a Windows Explorer plugin.	2009-02-08	<a href="#">9.3</a>	<a href="#">CVE-2009-0375</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
realnetworks -- realplayer	A DLL file in RealNetworks RealPlayer 11 allows remote attackers to execute arbitrary code via a crafted Internet Video Recording (IVR) file with a modified field that controls an unspecified structure length and triggers heap corruption, related to use of RealPlayer through a Windows Explorer plugin.	2009-02-08	<a href="#">9.3</a>	<a href="#">CVE-2009-0376</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a>
research_in_motion_limited -- blackberry_application_web_loader	Buffer overflow in the Research in Motion RIM AxLoader ActiveX control in AxLoader.ocx and AxLoader.dll in BlackBerry Application Web Loader 1.0 allows remote attackers to execute arbitrary code via unspecified vectors.	2009-02-10	<a href="#">9.3</a>	<a href="#">CVE-2009-0305</a> <a href="#">CONFIRM</a>
rhadrix -- if-cms	SQL injection vulnerability in frame.php in Rhadrix If-CMS 2.07 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2009-0528</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
rimarts. -- becky!_internet_mail	Buffer overflow in Becky! Internet Mail 2.48.02 and earlier allows remote attackers to execute arbitrary code via a mail message with a crafted return receipt request.	2009-02-12	<a href="#">9.3</a>	<a href="#">CVE-2009-0569</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a> <a href="#">IVNDB</a> <a href="#">JVN</a>
rportal -- rportal	PHP remote file inclusion vulnerability in index.php in RPortal 1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the file_op parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2008-6099</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a>
	Unspecified vulnerability in SemanticScuttle before 2009-02-	2009-02-		<a href="#">CVE-2008-6110</a>

semanticscuttle -- semanticscuttle	0.90 has unknown impact and attack vectors related to improper validation of parameters to profile.php.	2009-02-10	<a href="#">10.0</a>	<a href="#">CONFIRM SECUNIA</a>
simpleircbot -- simpleircbot	Unspecified vulnerability in SimpleIrcBot before 1.0 Stable has unknown impact and attack vectors related to an "auth vulnerability."	2009-02-09	<a href="#">10.0</a>	<a href="#">CVE-2009-0492 BID</a>
sirini -- grboard	Multiple PHP remote file inclusion vulnerabilities in GRBoard 1.8, when register_globals is enabled and magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) theme parameter to (a) 179_squarebox_pds_list/view.php, (b) 179_squarebox_minishop_expand/view.php, (c) 179_squarebox_gallery_list_pds/view.php, (d) 179_squarebox_gallery_list/view.php, (e) 179_squarebox_gallery/view.php, (f) 179_squarebox_board_swfupload/view.php, (g) 179_squarebox_board_expand/view.php, (h) 179_squarebox_board_basic_with_grcode/view.php, (i) 179_squarebox_board_basic/view.php, (j) 179_simplebar_pds_list/view.php, (k) 179_simplebar_notice/view.php, (l) 179_simplebar_gallery_list_pds/view.php, (m) 179_simplebar_gallery/view.php, and (n) 179_simplebar_basic/view.php in theme/; the (2) path parameter to (o) latest/sirini_gallery_latest/list.php; and the (3) grboard parameter to (p) include.php and (q) form_mail.php.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0444 MILWORM SECUNIA</a>
skalinks -- skalinks	SQL injection vulnerability in Skalfa SkaLinks 1.5 allows remote attackers to execute arbitrary SQL commands via the Admin name field to the default URI under admin/.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0451 BID MILWORM</a>
socialengine -- socialengine	SQL injection vulnerability in profile_comments.php in SocialEngine (SE) 2.7 and earlier allows remote attackers to execute arbitrary SQL commands via the comment_secure parameter.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6120 XF BID BUGTRAQ</a>
socialengine -- socialengine	CRLF injection vulnerability in SocialEngine (SE) 2.7 and earlier allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the PHPSESSID cookie.	2009-02-11	<a href="#">7.5</a>	<a href="#">CVE-2008-6121 XF BID BUGTRAQ</a>
sourdough -- sourdough	PHP remote file inclusion vulnerability in examples/example_clientside_javascript.php in patForms, as used in Sourdough 0.3.5, allows remote attackers to execute arbitrary PHP code via a URL in the neededFiles[patForms] parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0456 BID MILWORM</a>
synactis -- all_in_the_box.ocx	The SaveDoc method in the All_In_The_Box.AllBox ActiveX control in ALL_IN_THE_BOX.OCX in Synactis ALL In-The-Box ActiveX 3 allows remote attackers to create and overwrite arbitrary files via an argument ending in a '\0' character, which bypasses the intended .box filename extension, as demonstrated by a C:\boot.ini\0 argument.	2009-02-10	<a href="#">9.3</a>	<a href="#">CVE-2009-0465 BID MILWORM MISC SECUNIA OSVDB</a>

syntax_desktop -- syntax_desktop	Directory traversal vulnerability in admin/modules/aa/preview.php in Syntax Desktop 2.7 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the synTarget parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0448</a> <a href="#">BID</a> <a href="#">MILWORM</a>
web-album -- webalbum	SQL injection vulnerability in photo.php in WEBAlbum 2.4b allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0446</a> <a href="#">BID</a> <a href="#">MILWORM</a>
web_design_hero -- joomladate	SQL injection vulnerability in the JoomlaDate (com_joomladate) component 1.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the user parameter in a viewProfile action to index.php.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2008-6068</a> <a href="#">XF</a> <a href="#">MILWORM</a>
webframe -- webframe	Multiple PHP remote file inclusion vulnerabilities in WebFrame 0.76 allow remote attackers to execute arbitrary PHP code via a URL in the classFiles parameter to (1) admin/doc/index.php, (2) index.php, and (3) base/menu.php in mod/.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0513</a> <a href="#">BID</a> <a href="#">MILWORM</a>
wholehogsoftware -- ware_support	Multiple SQL injection vulnerabilities in admin/login_submit.php in Whole Hog Ware Support 1.x allow remote attackers to execute arbitrary SQL commands via (1) the uid parameter (aka Username field) or (2) the pwd parameter (aka Password field). NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0458</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MILWORM</a>
wholehogsoftware -- password_protect	Multiple SQL injection vulnerabilities in admin/login_submit.php in Whole Hog Password Protect: Enhanced 1.x allow remote attackers to execute arbitrary SQL commands via (1) the uid parameter (aka Username field) or (2) the pwd parameter (aka Password field). NOTE: some of these details are obtained from third party information.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0459</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MILWORM</a>
wholehogsoftware -- ware_support	Whole Hog Ware Support 1.x allows remote attackers to bypass authentication and obtain administrative access via an integer value in the adminid cookie.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0460</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MILWORM</a>
wholehogsoftware -- password_protect	Whole Hog Password Protect: Enhanced 1.x allows remote attackers to bypass authentication and obtain administrative access via an integer value in the adminid cookie.	2009-02-10	<a href="#">7.5</a>	<a href="#">CVE-2009-0461</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MILWORM</a>
zeroshell -- zeroshell	cgi-bin/kerbynet in ZeroShell 1.0beta11 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in the type parameter in a NoAuthREQ x509List action.	2009-02-12	<a href="#">10.0</a>	<a href="#">CVE-2009-0545</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">FRSIRT</a>

[Back to top](#)**Medium Vulnerabilities**

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
				<a href="#">CVE 2009</a>

a4desk -- a4desk_flash_event_calendar	PHP remote file inclusion vulnerability in index.php in A4Desk Event Calendar, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via a URL in the v parameter.	2009-02-10	<a href="#">6.8</a>	<a href="#">CVE-2009-6103</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
adaptcms -- adaptcms	Multiple cross-site scripting (XSS) vulnerabilities in index.php in AdaptCMS Lite 1.4 allow remote attackers to inject arbitrary web script or HTML via the (1) url and (2) acuparam parameters, and (3) the URI.	2009-02-11	<a href="#">4.3</a>	<a href="#">CVE-2009-0526</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
adaptcms -- adaptcms	PHP remote file inclusion vulnerability in plugins/rss_importer_functions.php in AdaptCMS Lite 1.4 allows remote attackers to execute arbitrary PHP code via a URL in the sitepath parameter.	2009-02-11	<a href="#">6.8</a>	<a href="#">CVE-2009-0527</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
agavi -- agavi	Cross-site scripting (XSS) vulnerability in the AgaviWebRouting::gen(null) method in Agavi 0.11 before 0.11.6 and 1.0 before 1.0.0 beta 8 allows remote attackers to inject arbitrary web script or HTML via a crafted URL with certain characters that are not properly handled by web browsers that do not strictly follow RFC 3986, such as Internet Explorer 6 and 7.	2009-02-10	<a href="#">4.3</a>	<a href="#">CVE-2009-0417</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in the Pixlet codec in Apple Mac OS X 10.4.11 and 10.5.6 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via a crafted movie file that triggers memory corruption.	2009-02-12	<a href="#">6.8</a>	<a href="#">CVE-2009-0009</a> <a href="#">APPLE</a>
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in fsevents in the FSEvents framework in Apple Mac OS X 10.5.6 allows local users to obtain sensitive information (filesystem activities and directory names) via unknown vectors related to "credential management."	2009-02-12	<a href="#">4.9</a>	<a href="#">CVE-2009-0015</a> <a href="#">APPLE</a>
armorlogic -- profense_web_application_firewall	Cross-site scripting (XSS) vulnerability in proxy.html in Profense Web Application Firewall 2.6.2 and 2.6.3 allows remote attackers to inject arbitrary web script or HTML via the proxy parameter in a deny_log manage action.	2009-02-10	<a href="#">4.3</a>	<a href="#">CVE-2009-0467</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
armorlogic -- profense_web_application_firewall	Multiple cross-site request forgery (CSRF) vulnerabilities in ajax.html in Profense Web Application Firewall 2.6.2 and 2.6.3 allow remote attackers to (1) shutdown the server, (2) send ping packets, (3) enable network services, (4) configure a proxy server, and (5) modify other settings as administrators via parameters in the query string.	2009-02-10	<a href="#">6.8</a>	<a href="#">CVE-2009-0468</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
berlios -- discussion_forum_2k	Multiple SQL injection vulnerabilities in Discussion Forums 2k 3.3, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) CatID parameter to (a) RSS1.php and (b)	2009-02-10	<a href="#">6.8</a>	<a href="#">CVE-2008-6100</a> <a href="#">BID</a> <a href="#">MILWORM</a>

	RSS2.php in misc/; and the (2) SubID parameter to (c) misc/RSS5.php.			<a href="#">MILWORM</a>
bmforum -- bmforum	SQL injection vulnerability in plugins.php in BMForum 5.6, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the tagname parameter.	2009-02-09	<a href="#">6.8</a>	<a href="#">CVE-2008-6091</a> <a href="#">BID</a> <a href="#">MILWORM</a>
celoxis -- celoxis	Cross-site scripting (XSS) vulnerability in user.do in Celoxis Technologies Celoxis allows remote attackers to inject arbitrary web script or HTML via the ni.smessage parameter.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2008-6094</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">FULLDISC</a>
cisco -- ios	Multiple cross-site scripting (XSS) vulnerabilities in the HTTP server in Cisco IOS 12.4(23) allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to the default URI under (1) level/15/exec/- or (2) exec/, a different vulnerability than CVE-2008-3821.	2009-02-06	<a href="#">4.3</a>	<a href="#">CVE-2009-0470</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a>
cisco -- ios	Cross-site request forgery (CSRF) vulnerability in the HTTP server in Cisco IOS 12.4(23) allows remote attackers to execute arbitrary commands, as demonstrated by executing the hostname command with a level/15/configure/-/hostname request.	2009-02-06	<a href="#">6.8</a>	<a href="#">CVE-2009-0471</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a>
electrictoad -- snippetmaster_webpage_editor	Cross-site scripting (XSS) vulnerability in index.php in SnippetMaster Webpage Editor 2.2.2 allows remote attackers to inject arbitrary web script or HTML via the language parameter.	2009-02-11	<a href="#">4.3</a>	<a href="#">CVE-2009-0529</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
eset -- remote_administrator	Cross-site scripting (XSS) vulnerability in the Additional Report Settings interface in ESET Remote Administrator before 3.0.105 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: some of these details are obtained from third party information.	2009-02-12	<a href="#">4.3</a>	<a href="#">CVE-2009-0548</a> <a href="#">FRSIRT</a>
evolution -- evolution	Evolution 2.22.3.1 checks S/MIME signatures against a copy of the e-mail text within a signed-data blob, not the copy of the e-mail text displayed to the user, which allows remote attackers to spoof a signature by modifying the latter copy, a different vulnerability than CVE-2008-5077.	2009-02-12	<a href="#">5.0</a>	<a href="#">CVE-2009-0547</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>
eyrie -- pam-krb5	Russ Allbery pam-krb5 before 3.13, when linked against MIT Kerberos, does not properly initialize the Kerberos libraries for setuid use, which allows local users to gain privileges by pointing an environment variable to a modified Kerberos configuration file, and then launching a PAM-based setuid application.	2009-02-13	<a href="#">6.2</a>	<a href="#">CVE-2009-0360</a> <a href="#">FRSIRT</a>
eyrie -- pam-krb5	Russ Allbery pam-krb5 before 3.13, as used by libpam-heimdal, su in Solaris 10, and other software, does not properly handle calls to pam_setcred when running setuid, which allows local users to overwrite and change the ownership	2009-02-12	<a href="#">4.6</a>	<a href="#">CVE-2009-0361</a>

	of arbitrary files by setting the KRB5CCNAME environment variable, and then launching a setuid application that performs certain pam_setcred operations.	1.3		<a href="#">FRSIRT</a>
fail2ban -- fail2ban	filter.d/wuftpd.conf in Fail2ban 0.8.3 uses an incorrect regular expression that allows remote attackers to cause a denial of service (forced authentication failures) via a crafted reverse-resolved DNS name (rhost) entry that contains a substring that is interpreted as an IP address, a different vulnerability than CVE-2007-4321.	2009-02-12	4.0	<a href="#">CVE-2009-0362</a> <a href="#">BID</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a>
graphicsmagick -- graphicsmagick	Multiple unspecified vulnerabilities in GraphicsMagick before 1.1.14, and 1.2.x before 1.2.3, allow remote attackers to cause a denial of service (crash) via unspecified vectors in (1) XCF and (2) CINEON images.	2009-02-10	5.0	<a href="#">CVE-2008-6072</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
groonesworld -- gbook	PHP remote file inclusion vulnerability in includes/header.php in Groone GBook 2.0 allows remote attackers to execute arbitrary PHP code via a URL in the abspath parameter.	2009-02-10	5.1	<a href="#">CVE-2009-0464</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
gwm -- galatolo_webmanager	Cross-site scripting (XSS) vulnerability in result.php in Galatolo WebManager (GWM) 1.0 allows remote attackers to inject arbitrary web script or HTML via the key parameter.	2009-02-10	4.3	<a href="#">CVE-2008-6108</a> <a href="#">MILWORM</a>
hp -- oncplus	Unspecified vulnerability in NFS in HP ONCplus B.11.31.05 and earlier for HP-UX B.11.31 allows local users to cause a denial of service via unknown vectors.	2009-02-08	4.9	<a href="#">CVE-2009-0206</a> <a href="#">HP</a>
ibm -- workplace_for_business_controls_and_reporting ibm -- workplace_web_content_management	Cross-site scripting (XSS) vulnerability in IBM Workplace for Business Controls and Reporting 2.x and IBM Workplace Web Content Management 6.x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: some of these details are obtained from third party information.	2009-02-10	4.3	<a href="#">CVE-2008-6105</a> <a href="#">BID</a> <a href="#">AIXAPAR</a> <a href="#">SECUNIA</a>
ibm -- workplace_for_business_controls_and_reporting ibm -- workplace_web_content_management	Cross-site request forgery (CSRF) vulnerability in IBM Workplace for Business Controls and Reporting 2.x and IBM Workplace Web Content Management 6.x has unknown impact and remote attack vectors. NOTE: some of these details are obtained from third party information.	2009-02-10	6.8	<a href="#">CVE-2008-6106</a> <a href="#">AIXAPAR</a> <a href="#">SECUNIA</a>
ibm -- websphere_application_server	Open redirect vulnerability in the ibm_security_logout servlet in IBM WebSphere Application Server (WAS) 5.1.1.19 and earlier 5.x versions, 6.0.x before 6.0.2.33, and 6.1.x before 6.1.0.23 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the logoutExitPage feature.	2009-02-10	5.8	<a href="#">CVE-2008-4284</a> <a href="#">AIXAPAR</a> <a href="#">CONFIRM</a>
ibm -- websphere_application_server	The installation process for the File Transfer servlet in the System Management/Repository component in IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.19 does not enable the secure version, which allows remote attackers to obtain sensitive information via unspecified	2009-02-10	5.0	<a href="#">CVE-2009-0432</a> <a href="#">CONFIRM</a>

	vectors.			
ibm -- websphere_application_server	Unspecified vulnerability in the IBM Asynchronous I/O (aka AIO or libibmaio) library in the Java Message Service (JMS) component in IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.17 on AIX 5.3 allows attackers to cause a denial of service (daemon crash) via vectors related to the aio_getioev2 and getEvent methods.	2009-02-10	<a href="#">5.0</a>	<a href="#">CVE-2009-0435</a> <a href="#">CONFIRM</a> <a href="#">AIXAPAR</a>
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 7 before 7.0.0.1 on Windows allows remote attackers to bypass "Authorization checking" and obtain sensitive information from JSP pages via a crafted request. NOTE: this is probably a duplicate of CVE-2008-5412.	2009-02-10	<a href="#">5.0</a>	<a href="#">CVE-2009-0438</a> <a href="#">CONFIRM</a>
ibm -- aix	at in bos.rte.cron on IBM AIX 5.2.0, 5.3.0 through 5.3.9, and 6.1.0 through 6.1.2 allows local users to read arbitrary files via unspecified vectors, related to failure to drop root privileges.	2009-02-11	<a href="#">4.9</a>	<a href="#">CVE-2009-0536</a> <a href="#">BID</a> <a href="#">CONFIRM</a>
ignite_realtime -- openfire	Multiple cross-site scripting (XSS) vulnerabilities in Ignite Realtime Openfire 3.6.2 allow remote attackers to inject arbitrary web script or HTML via the (1) log parameter to (a) logviewer.jsp and (b) log.jsp; (2) search parameter to (c) group-summary.jsp; (3) username parameter to (d) user-properties.jsp; (4) logDir, (5) maxTotalSize, (6) maxFileSize, (7) maxDays, and (8) logTimeout parameters to (e) audit-policy.jsp; (9) propName parameter to (f) server-properties.jsp; and the (10) roomconfig_roomname and (11) roomconfig_roomdesc parameters to (g) muc-room-edit-form.jsp. NOTE: this can be leveraged for arbitrary code execution by using XSS to upload a malicious plugin.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2009-0496</a> <a href="#">CONFIRM</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">CONFIRM</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
ignite_realtime -- openfire	Directory traversal vulnerability in log.jsp in Ignite Realtime Openfire 3.6.2 allows remote attackers to read arbitrary files via a ..\ (dot dot backslash) in the log parameter.	2009-02-09	<a href="#">5.0</a>	<a href="#">CVE-2009-0497</a> <a href="#">MISC</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
juniper -- netscreen_screenos juniper -- netscreen_screenos	Cross-site scripting (XSS) vulnerability in Juniper NetScreen ScreenOS before 5.4r10, 6.0r6, and 6.1r2 allows remote attackers to inject arbitrary web script or HTML via the user name parameter to the (1) web interface login page or the (2) telnet login page.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2008-6096</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">FRSIRT</a> <a href="#">SECUNIA</a>
libvirt libvirt	Buffer overflow in the proxyReadClientSocket function in proxy/libvirt_proxy.c in libvirt_proxy 0.5.1 might allow local users to gain privileges by sending a portion of the header of a	2009-02-	<a href="#">4.4</a>	<a href="#">CVE-2009-0036</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">MTIIST</a>

linux -- linux	virProxyPacket packet, and then sending the remainder of the packet with crafted values in the header, related to use of uninitialized memory in a validation check.	11	<a href="#">+/-</a>	<a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">BID</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
linux -- kernel	The (1) sys32_mremap function in arch/sparc64/kernel/sys_sparc32.c, the (2) sparc_mmap_check function in arch/sparc/kernel/sys_sparc.c, and the (3) sparc64_mmap_check function in arch/sparc64/kernel/sys_sparc.c, in the Linux kernel before 2.6.25.4, omit some virtual-address range (aka span) checks when the mremap MREMAP_FIXED bit is not set, which allows local users to cause a denial of service (panic) via unspecified mremap calls, a related issue to CVE-2008-2137.	2009-02-10	<a href="#">4.9</a>	<a href="#">CVE-2008-6107</a> <a href="#">CONFIRM</a> <a href="#">SECTRACK</a> <a href="#">MLIST</a>
magic2003 -- storagecrypt	StorageCrypt 2.0.1 does not properly encrypt disks, which allows local users to obtain sensitive information via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-10	<a href="#">4.9</a>	<a href="#">CVE-2008-6073</a> <a href="#">SECUNIA</a>
mahara -- mahara	Cross-site scripting (XSS) vulnerability in Mahara before 1.0.9 allows remote attackers to inject arbitrary web script or HTML via a crafted forum post.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2009-0487</a> <a href="#">CONFIRM</a>
microsoft -- exchange_server	The Electronic Messaging System Microsoft Data Base (EMSMDB32) provider in Microsoft Exchange 2000 Server SP3 and Exchange Server 2003 SP2, as used in Exchange System Attendant, allows remote attackers to cause a denial of service (application outage) via a malformed MAPI command, aka "Literal Processing Vulnerability."	2009-02-10	<a href="#">5.0</a>	<a href="#">CVE-2009-0099</a> <a href="#">MS</a>
minitdesign -- virtual_guestbook	Virtual GuestBook (vgbook) 2.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request to guestbook.mdb.	2009-02-09	<a href="#">5.0</a>	<a href="#">CVE-2009-0498</a> <a href="#">MILWORM</a>
modernmethod -- sajax	Cross-site scripting (XSS) vulnerability in the sajax_get_common_js function in php/Sajax.php in Sajax 0.12 allows remote attackers to inject arbitrary web script or HTML via the URL parameter, which is not properly handled when using browsers that do not URL-encode requests, such as Internet Explorer 6. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-11	<a href="#">4.3</a>	<a href="#">CVE-2009-0525</a> <a href="#">BID</a> <a href="#">SECUNIA</a>
moodle -- moodle	Cross-site request forgery (CSRF) vulnerability in the forum code in Moodle 1.7 before 1.7.7, 1.8 before 1.8.8, and 1.9 before 1.9.4 allows remote attackers to delete unauthorized forum posts via a link or IMG tag to post.php.	2009-02-09	<a href="#">6.4</a>	<a href="#">CVE-2009-0499</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
	Cross-site scripting (XSS) vulnerability in course/lib.php in Moodle 1.6 before 1.6.9, 1.7			<a href="#">CVE-2009-</a>

moodle -- moodle	before 1.7.7, 1.8 before 1.8.8, and 1.9 before 1.9.4 allows remote attackers to inject arbitrary web script or HTML via crafted log table information that is not properly handled when it is displayed in a log report.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2009-0500</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
moodle -- moodle	Unspecified vulnerability in the Calendar export feature in Moodle 1.8 before 1.8.8 and 1.9 before 1.9.4 allows attackers to obtain sensitive information and conduct "brute force attacks on user accounts" via unknown vectors.	2009-02-09	<a href="#">5.0</a>	<a href="#">CVE-2009-0501</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
moodle -- moodle snoopy -- snoopy	Cross-site scripting (XSS) vulnerability in blocks/html/block_html.php in Snoopy 1.2.3, as used in Moodle 1.6 before 1.6.9, 1.7 before 1.7.7, 1.8 before 1.8.8, and 1.9 before 1.9.4, allows remote attackers to inject arbitrary web script or HTML via an HTML block, which is not properly handled when the "Login as" feature is used to visit a MyMoodle or Blog page.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2009-0502</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
moodle -- moodle	Unspecified vulnerability in the user editing interface in Moodle 1.5.x, 1.6 before 1.6.6, and 1.7 before 1.7.3 allows remote authenticated users to gain privileges via unknown vectors.	2009-02-12	<a href="#">6.5</a>	<a href="#">CVE-2008-6125</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Cross-site request forgery (CSRF) vulnerability in Bugzilla before 3.2 before 3.2.1, 3.3 before 3.3.2, and other versions before 3.2 allows remote attackers to perform bug updating activities as other users via a link or IMG tag to process_bug.cgi.	2009-02-09	<a href="#">5.8</a>	<a href="#">CVE-2009-0482</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Cross-site request forgery (CSRF) vulnerability in Bugzilla 2.22 before 2.22.7, 3.0 before 3.0.7, 3.2 before 3.2.1, and 3.3 before 3.3.2 allows remote attackers to delete keywords and user preferences via a link or IMG tag to (1) editkeywords.cgi or (2) userprefs.cgi.	2009-02-09	<a href="#">5.8</a>	<a href="#">CVE-2009-0483</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Cross-site request forgery (CSRF) vulnerability in Bugzilla 3.0 before 3.0.7, 3.2 before 3.2.1, and 3.3 before 3.3.2 allows remote attackers to delete shared or saved searches via a link or IMG tag to buglist.cgi.	2009-02-09	<a href="#">5.8</a>	<a href="#">CVE-2009-0484</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Cross-site request forgery (CSRF) vulnerability in Bugzilla 2.17 to 2.22.7, 3.0 before 3.0.7, 3.2 before 3.2.1, and 3.3 before 3.3.2 allows remote attackers to delete unused flag types via a link or IMG tag to editflagtypes.cgi.	2009-02-09	<a href="#">5.8</a>	<a href="#">CVE-2009-0485</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
mozilla -- bugzilla	Bugzilla 3.2 before 3.2 RC2, 3.0 before 3.0.6, 2.22 before 2.22.6, 2.20 before 2.20.7, and other versions after 2.17.4 allows remote authenticated users to bypass moderation to approve and disapprove quips via a direct request to quips.cgi with the action parameter set to "approve."	2009-02-09	<a href="#">4.0</a>	<a href="#">CVE-2008-6098</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>
net-snmp -- net-snmp net-snmp -- net_snmp	The netsnmp_udp_fmtaddr function (snmplib/snmpUDPDomain.c) in net-snmp 5.0.9 through 5.4.2, when using TCP wrappers for client authorization, does not properly parse hosts.allow rules, which allows remote attackers to bypass	2009-02-12	<a href="#">5.0</a>	<a href="#">CVE-2008-6123</a> <a href="#">CONFIRM</a> <a href="#">MLIST</a>

	intended access restrictions and execute SNMP queries, related to "source/destination IP address confusion."		<a href="#">CONFIRM</a> <a href="#">MISC</a>
noname-cms -- noname_cms	SQL injection vulnerability in index.php in Noname CMS 1.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the (1) file_id parameter in a detailansicht action and the (2) kategorie parameter in a kategorien action.	2009-02-09	<a href="#">6.8</a> <a href="#">CVE-2008-6093</a> <a href="#">BID</a> <a href="#">MILWORM</a>
onlinegrades -- online_grades	Multiple SQL injection vulnerabilities in parents/login.php in Online Grades 3.2.4, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) uname or (2) pass parameter.	2009-02-10	<a href="#">6.8</a> <a href="#">CVE-2009-0452</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
onlinegrades -- online_grades	Online Grades 3.2.4 allows remote attackers to obtain configuration information via a direct request to phpinfo.php, which calls the phpinfo function.	2009-02-10	<a href="#">5.0</a> <a href="#">CVE-2009-0453</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
opennms -- opennms	Cross-site scripting (XSS) vulnerability in surveillanceView.htm in OpenNMS 1.5.94 allows remote attackers to inject arbitrary web script or HTML via the viewName parameter.	2009-02-09	<a href="#">4.3</a> <a href="#">CVE-2008-6095</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>
phorum -- phorum	Cross-site scripting (XSS) vulnerability in Phorum before 5.2.10 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-02-09	<a href="#">4.3</a> <a href="#">CVE-2009-0488</a> <a href="#">CONFIRM</a>
phpbbbook -- phpbbbook	Directory traversal vulnerability in bbcode.php in PHPbbBook 1.3 and 1.3h allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the l parameter.	2009-02-10	<a href="#">6.8</a> <a href="#">CVE-2009-0442</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
proftpd -- proftpd	ProFTPD Server 1.3.1, with NLS support enabled, allows remote attackers to bypass SQL injection protection mechanisms via invalid, encoded multibyte characters, which are not properly handled in (1) mod_sql_mysql and (2) mod_sql_postgres.	2009-02-12	<a href="#">6.8</a> <a href="#">CVE-2009-0543</a> <a href="#">MLIST</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a>
scripts_for_sites -- ez_baby	Cross-site scripting (XSS) vulnerability in password.php in Scripts For Sites (SFS) EZ Baby allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-11	<a href="#">4.3</a> <a href="#">CVE-2009-0532</a> <a href="#">XF</a> <a href="#">BID</a>
scripts_for_sites -- ez_reminder	Cross-site scripting (XSS) vulnerability in password.php in Scripts for Sites EZ Reminder allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-11	<a href="#">4.3</a> <a href="#">CVE-2009-0533</a> <a href="#">XF</a> <a href="#">BID</a>

scriptsez -- ez_ringtone_manager	Multiple directory traversal vulnerabilities in Ez Ringtone Manager allow remote attackers to read arbitrary files via a .. (dot dot) in the id parameter in a detail action to (1) main.php and (2) template.php in ringtones/.	2009-02-11	<a href="#">5.0</a>	<a href="#">CVE-2008-6112</a> <a href="#">BID</a> <a href="#">MILWORM</a>
semanticscuttle -- semanticscuttle	Cross-site scripting (XSS) vulnerability in SemanticScuttle before 0.90 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to the (1) username and (2) profile page.	2009-02-11	<a href="#">4.3</a>	<a href="#">CVE-2008-6113</a> <a href="#">BID</a>
shelter_manager -- animal_shelter_manager	Robin Rawson-Tetley Animal Shelter Manager (ASM) before 2.2.2 does not properly enforce the privileges of user accounts, which allows local users to bypass intended access restrictions by (1) opening unspecified screens, related to the "double click selector bug"; or modifying a (2) animal, (3) owner, (4) lost/found, (5) diary note, (6) owner donation, or (7) waiting list record, related to "change permissions" and the "new UI."	2009-02-10	<a href="#">4.6</a>	<a href="#">CVE-2008-6109</a> <a href="#">XF</a>
squid -- squid	Squid 2.7 to 2.7.STABLE5, 3.0 to 3.0.STABLE12, and 3.1 to 3.1.0.4 allows remote attackers to cause a denial of service via an HTTP request with an invalid version number, which triggers a reachable assertion in (1) HttpMsg.c and (2) HttpStatusLine.c.	2009-02-08	<a href="#">5.0</a>	<a href="#">CVE-2009-0478</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">SECTRACK</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
technote -- technote	PHP remote file inclusion vulnerability in skin_shop/standard/2_view_body/body_default.php in Technote 7.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the shop_this_skin_path parameter, a different vector than CVE-2008-4138.	2009-02-10	<a href="#">6.8</a>	<a href="#">CVE-2009-0441</a> <a href="#">BID</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a>
vivvo -- vivvo	Cross-site scripting (XSS) vulnerability in Vivvo CMS before 4.1.1 allows remote attackers to inject arbitrary web script or HTML via a URI that triggers a 404 Page Not Found response.	2009-02-10	<a href="#">4.3</a>	<a href="#">CVE-2009-0466</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a>
wikyblog -- wikyblog	Multiple cross-site scripting (XSS) vulnerabilities in WikyBlog before 1.7.1 allow remote attackers to inject arbitrary web script or HTML via the (1) key parameter to index.php/Special/Main/keywordSearch, (2) revNum parameter to index.php/Edit/Main/Home, (3) to parameter to index.php/Special/Main/WhatLinksHere, (4) user parameter to index.php/Special/Main/UserEdits, and (5) the PATH_INFO to index.php.	2009-02-09	<a href="#">4.3</a>	<a href="#">CVE-2008-6097</a> <a href="#">BID</a> <a href="#">MISC</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
yanocc -- yanocc	Directory traversal vulnerability in check_lang.php in Yet Another NOCC (YANOCC) 0.1.0 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	2009-02-10	<a href="#">6.8</a>	<a href="#">CVE-2009-0515</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MILWORM</a>

[Back to top](#)

<b>Low Vulnerabilities</b>					
<b>Primary Vendor -- Product</b>	<b>Description</b>	<b>Published</b>	<b>CVSS Score</b>	<b>Source &amp; Patch Info</b>	
apple -- mac_os_x apple -- mac_os_x_server	Race condition in AFP Server in Apple Mac OS X 10.5.6 allows local users to cause a denial of service (infinite loop) via unspecified vectors related to "file enumeration logic."	2009-02-12	<a href="#">1.9</a>	<a href="#">CVE-2009-0142</a> <a href="#">APPLE</a>	
apple -- mac_os_x apple -- mac_os_x_server	dscl in DS Tools in Apple Mac OS X 10.4.11 and 10.5.6 requires that passwords must be provided as command line arguments, which allows local users to gain privileges by listing process information.	2009-02-12	<a href="#">2.1</a>	<a href="#">CVE-2009-0013</a> <a href="#">APPLE</a>	
apple -- mac_os_x apple -- mac_os_x_server	Folder Manager in Apple Mac OS X 10.5.6 uses insecure default permissions when recreating a Downloads folder after it has been deleted, which allows local users to bypass intended access restrictions and read the Downloads folder.	2009-02-12	<a href="#">2.1</a>	<a href="#">CVE-2009-0014</a> <a href="#">APPLE</a>	
apple -- mac_os_x apple -- mac_os_x_server	XTerm in Apple Mac OS X 10.4.11 and 10.5.6, when used with luit, creates tty devices with insecure world-writable permissions, which allows local users to write to the Xterm of another user.	2009-02-12	<a href="#">2.1</a>	<a href="#">CVE-2009-0141</a> <a href="#">APPLE</a>	
glfusion -- glfusion	Cross-site scripting (XSS) vulnerability in the anonymous comments feature in lib-comment.php in glFusion 1.1.0, 1.1.1, and earlier versions allows remote attackers to inject arbitrary web script or HTML via the username parameter to comment.php.	2009-02-10	<a href="#">2.6</a>	<a href="#">CVE-2009-0455</a> <a href="#">BID</a>	
ibm -- websphere_application_server	Unspecified vulnerability in IBM WebSphere Application Server (WAS) 5.1.x before 5.1.1.19, 6.0.x before 6.0.2.29, and 6.1.x before 6.1.0.19, when Web Server plug-in content buffering is enabled, allows attackers to cause a denial of service (daemon crash) via unknown vectors, related to a mishandling of client read failures in which clients receive many 500 HTTP error responses and backend servers are incorrectly labeled as down.	2009-02-10	<a href="#">2.6</a>	<a href="#">CVE-2009-0433</a> <a href="#">BID</a> <a href="#">AIXAPAR</a> <a href="#">CONFIRM</a>	
ibm -- websphere_application_server	PerfServlet in the PMI/Performance Tools component in IBM WebSphere Application Server (WAS) 6.0.x before 6.0.2.31, 6.1.x before 6.1.0.21, and 7.0.x before 7.0.0.1, when Performance Monitoring Infrastructure (PMI) is enabled, allows local users to obtain sensitive information by reading the (1) systemout.log and (2) ffdc files. NOTE: this is probably a duplicate of CVE-2008-5413.	2009-02-10	<a href="#">1.9</a>	<a href="#">CVE-2009-0434</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">AIXAPAR</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a> <a href="#">MISC</a>	
ibm -- websphere_application_server	The Installation Factory installation process for IBM WebSphere Application Server (WAS) 6.0.2 on Windows, when WAS is registered as a Windows service, allows local users to obtain sensitive information by	2009-02-10	<a href="#">1.9</a>	<a href="#">CVE-2009-0437</a> <a href="#">XF</a>	

	reading the logs/instconfigifwas6.log log file.			
mozilla -- bugzilla	Bugzilla 2.x before 2.22.7, 3.0 before 3.0.7, 3.2 before 3.2.1, and 3.3 before 3.3.2 allows remote authenticated users to conduct cross-site scripting (XSS) and related attacks by uploading HTML and JavaScript attachments that are rendered by web browsers.	2009-02-09	<a href="#">3.5</a>	<a href="#">CVE-2009-0481</a> <a href="#">CONFIRM</a>
wicd -- wicd	The DBus configuration file for Wicd before 1.5.9 allows arbitrary users to own org.wicd.daemon, which allows local users to receive messages that were intended for the Wicd daemon, possibly including credentials.	2009-02-09	<a href="#">2.1</a>	<a href="#">CVE-2009-0489</a> <a href="#">MLIST</a> <a href="#">CONFIRM</a> <a href="#">CONFIRM</a>

[Back to top](#)