

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
activewebsoftwares -- active_bids	Multiple SQL injection vulnerabilities in Active Bids allow remote attackers to execute arbitrary SQL commands via the (1) search parameter to search.asp, (2) SortDir parameter to auctionsended.asp, and the (3) catid parameter to wishlist.php.	2009-02-04	7.5	CVE-2009-0429 BID BUGTRAQ
adbnewssender -- adbnewssender	SQL injection vulnerability in ADbNewsSender before 1.5.2 allows remote attackers to execute arbitrary SQL commands via unspecified vectors in (1) opt_in_out.php.inc, (2) confirmation.php.inc, and (3) renewal.php.inc in mailinglist/.	2009-02-04	7.5	CVE-2008-6046 BID
agares_media -- arcadem_pro	SQL injection vulnerability in index.php in Arcadem Pro 2.700 through 2.802 allows remote attackers to execute arbitrary SQL commands via the articlecat parameter, probably related to includes/articleblock.php.	2009-02-03	7.5	CVE-2008-6040 MISC
attachmate -- reflection_for_secure_it	Multiple unspecified vulnerabilities in Attachmate Reflection for Secure IT UNIX Client and Server before 7.0 SP1 have unknown impact and attack vectors, aka "security vulnerabilities found by 3rd party analysis."	2009-02-02	10.0	CVE-2008-6021 CONFIRM
availscript -- availscript_article_script	SQL injection vulnerability in view.php in AvailScript Article Script allows remote attackers to execute arbitrary SQL commands via the v parameter.	2009-02-03	7.5	CVE-2008-6037 XF BID MILWORM
	PHP remote file inclusion vulnerability in main.inc.php in BaseBuilder 2.0.1 and earlier	2009-02-03		CVE-2008-6036

basebuilder -- basebuilder	allows remote attackers to execute arbitrary PHP code via a URL in the mj_config[src_path] parameter.	2009-02-03	7.5	BID MILWORM FRSIRT
blue_eye_cms -- blue_eye_cms	SQL injection vulnerability in index.php in Blue Eye CMS 1.0.0 and earlier allows remote attackers to execute arbitrary SQL commands via the clanek parameter.	2009-02-04	7.5	CVE-2009-0425 BID MILWORM
bluecube -- bluecube_cms	SQL injection vulnerability in tienda.php in BlueCUBE CMS allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-03	7.5	CVE-2008-6026 BID SECUNIA MISC
chipmunk_scripts -- chipmunk_blogger	Chipmunk Blogger Script allows remote attackers to gain administrator privileges via a direct request to admin/reguser.php. NOTE: this is only a vulnerability when the administrator does not properly follow installation directions.	2009-02-03	7.5	CVE-2009-0399 MILWORM
chipmunk_scripts -- chipmunk_blogger	SQL injection vulnerability in admin/authenticate.php in Chipmunk Blogger Script allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-02-03	7.5	CVE-2009-0403 XF MILWORM FRSIRT
cisco -- 4400_wireless_lan_controller cisco -- catalyst_3750_series_integrated_wireless_lan_controller cisco -- catalyst_6500_series_integrated_wireless_lan_controller cisco -- catalyst_7600_series_wireless_lan_controller cisco -- wireless_lan_controller	The Cisco Wireless LAN Controller (WLC), Cisco Catalyst 6500 Wireless Services Module (WiSM), and Cisco Catalyst 3750 Integrated Wireless LAN Controller with software 4.x before 4.2.176.0 and 5.2.x before 5.2.157.0 allow remote attackers to cause a denial of service (device reload) via a web authentication (aka WebAuth) session that includes a malformed POST request to login.html.	2009-02-04	7.8	CVE-2009-0059 CISCO
cisco -- 4400_wireless_lan_controller cisco -- catalyst_3750_series_integrated_wireless_lan_controller cisco -- catalyst_6500_series_integrated_wireless_lan_controller cisco -- catalyst_7600_series_wireless_lan_controller cisco -- wireless_lan_controller	Unspecified vulnerability in the Wireless LAN Controller (WLC) TSEC driver in the Cisco 4400 WLC, Cisco Catalyst 6500 and 7600 Wireless Services Module (WiSM), and Cisco Catalyst 3750 Integrated Wireless LAN Controller with software 4.x before 4.2.176.0 and 5.x before 5.1 allows remote attackers to cause a denial of service (device crash or hang) via unknown IP packets.	2009-02-04	7.8	CVE-2009-0061 CISCO
cisco -- catalyst_3750_series_integrated_wireless_lan_controller cisco -- catalyst_6500_wireless_services_modules cisco -- wireless_lan_controller	Unspecified vulnerability in the Cisco Wireless LAN Controller (WLC), Cisco Catalyst 6500 Wireless Services Module (WiSM), and Cisco Catalyst 3750 Integrated Wireless LAN Controller with software 4.2.173.0 allows remote authenticated users to gain privileges via unknown vectors, as demonstrated by escalation from the (1) Lobby Admin and (2) Local Management User privilege levels.	2009-02-04	9.0	CVE-2009-0062 CISCO
codefixer -- linkspro	SQL injection vulnerability in Default.asp in LinksPro Standard Edition allows remote attackers to execute arbitrary SQL commands via the OrderDirection parameter.	2009-02-04	7.5	CVE-2009-0431 BID MISC

community_cms -- community_cms	SQL injection vulnerability in index.php in Community CMS 0.4 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-03	7.5	CVE-2009-0406 XF BID MILWORM
dmxready -- classified_listings_manager	SQL injection vulnerability in CategoryManager/upload_image_category.asp in DMXReady Classified Listings Manager 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-02-04	7.5	CVE-2009-0426 XF BID SECUNIA MILWORM
dmxready -- directory_manager	SQL injection vulnerability in CategoryManager/upload_image_category.asp in DMXReady Member Directory Manager 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-02-04	7.5	CVE-2009-0427 XF BID SECUNIA MILWORM CONFIRM CONFIRM
dmxready -- secure_document_library	SQL injection vulnerability in CategoryManager/upload_image_category.asp in DMXReady Secure Document Library 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-02-04	7.5	CVE-2009-0428 XF BID SECUNIA MILWORM CONFIRM CONFIRM
do-cms -- do-cms	SQL injection vulnerability in index.php in EACOMM DO-CMS 3.0 allows remote attackers to execute arbitrary SQL commands via the p parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-02	7.5	CVE-2008-6019 XF BID
drupal -- views	SQL injection vulnerability in the Views module 6.x before 6.x-2.2 for Drupal allows remote attackers to execute arbitrary SQL commands via unspecified vectors related to "an exposed filter on CCK text fields."	2009-02-02	7.5	CVE-2008-6020 BID CONFIRM
enlightenment -- imlib2	Multiple unspecified vulnerabilities in imlib2 before 1.4.2 have unknown impact and attack vectors.	2009-02-06	10.0	CVE-2008-6079 BID FRSIRT CONFIRM SECUNIA
enomaly -- elastic_computing_platform	Argument injection vulnerability in Enomaly Elastic Computing Platform (ECP), formerly Enomalism, before 2.1.1 allows local users to send signals to arbitrary processes by populating the /tmp/enomalism2.pid file with command-line arguments for the kill program.	2009-02-02	7.2	CVE-2009-0390 BUGTRAQ
ephpscripts -- e-php_cms	SQL injection vulnerability in browssecats.php in E-Php CMS allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-02-03	7.5	CVE-2009-0401 XF BID MISC

ephpscripts -- e-shop_shopping_cart	SQL injection vulnerability in search_results.php in E-Shop Shopping Cart (aka E-Php Shopping Cart) allows remote attackers to execute arbitrary SQL commands via the cid parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-04	7.5	CVE-2008-6067 MISC BID SECUNIA
eztools-software -- web_on_windows_activedx	Multiple insecure method vulnerabilities in the Web On Windows (WOW) ActiveX control in WOW ActiveX 2 allow remote attackers to (1) create and overwrite arbitrary files via the WriteIniFileString method, (2) execute arbitrary programs via the ShellExecute method, (3) read from the registry via unspecified vectors, and (4) write to the registry via unspecified vectors. NOTE: vectors 1 and 2 can be used together to execute arbitrary code.	2009-02-02	9.3	CVE-2009-0389 XF BID MILWORM
f-secure -- f-secure_anti-virus f-secure -- f-secure_anti-virus_for_citrix_servers f-secure -- f-secure_anti-virus_for_microsoft_exchange f-secure -- f-secure_anti-virus_for_mimesweeper f-secure -- f-secure_anti-virus_for_windows_servers f-secure -- f-secure_anti-virus_for_workstations f-secure -- f-secure_anti-virus_linux_client_security f-secure -- f-secure_anti-virus_linux_server_security f-secure -- f-secure_client_security f-secure -- f-secure_home_server_security f-secure -- f-secure_internet_gatekeeper_for_linux f-secure -- f-secure_internet_gatekeeper_for_windows f-secure -- f-secure_internet_security f-secure -- f-secure_linux_security f-secure -- f-secure.messaging_security_gateway f-secure -- f-secure_protection_service_for_business f-secure -- f-secure_protection_service_for_consumers	Integer overflow in multiple F-Secure anti-virus products, including Internet Security 2006 through 2008, Anti-Virus 2006 through 2008, and others, when configured to scan inside compressed archives, allows remote attackers to execute arbitrary code via a crafted RPM compressed archive file, which triggers a buffer overflow.	2009-02-06	7.6	CVE-2008-6085 CONFIRM
free_download_manager -- free_download_manager	Stack-based buffer overflow in Remote Control Server in Free Download Manager (FDM) 2.5 Build 758 and 3.0 Build 844 allows remote attackers to execute arbitrary code via a long Authorization header in an HTTP request.	2009-02-03	10.0	CVE-2009-0183 BID BUGTRAQ FRSIRT MISC SECUNIA
free_download_manager -- free_download_manager	Multiple buffer overflows in the torrent parsing implementation in Free Download Manager (FDM) 2.5 Build 758 and 3.0 Build 844 allow remote attackers to execute arbitrary code via (1) a long file name within a torrent file, (2) a long tracker URL in a torrent file, or (3) a long comment in a torrent file.	2009-02-03	9.3	CVE-2009-0184 FRSIRT
gplhost -- domain_technologie_control	SQL injection vulnerability in client/new_account.php in Domain Technologie Control (DTC) before 0.29.16 allows remote attackers to execute arbitrary SQL commands via the (1) familyname, (2) christname, (3) company_name, (4) is_company, (5) email, (6) phone, (7) fax, (8)	2009-02-03	7.5	CVE-2009-0402 XF BID SECUNIA CONFIRM

	addr1, (9) addr2, (10) addr3, (11) zipcode, (12) city, (13) state, (14) country, and (15) vat_num parameters.			CONFIRM
gstreamer -- good_plug-ins gstreamer -- plug-ins	Heap-based buffer overflow in the qtdemux_parse_samples function in gst/qtdemux/qtdemux.c in GStreamer Good Plug-ins (aka gst-plugins-good) 0.10.9 through 0.10.11, and GStreamer Plug-ins (aka gstreamer-plugins) 0.8.5, might allow remote attackers to execute arbitrary code via crafted Time-to-sample (aka stts) atom data in a malformed QuickTime media .mov file.	2009-02-03	9.3	CVE-2009-0397 BID
gstreamer -- plug-ins	Array index error in the gst_qtp_trak_handler function in gst/qtdemux/qtdemux.c in GStreamer Plug-ins (aka gstreamer-plugins) 0.6.0 allows remote attackers to have an unknown impact via a crafted QuickTime media file.	2009-02-03	9.3	CVE-2009-0398 MLIST
hp -- hp-ux	The IPv6 Neighbor Discovery Protocol (NDP) implementation in HP HP-UX B.11.11, B.11.23, and B.11.31 does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity), read private network traffic, and possibly execute arbitrary code via a spoofed message that modifies the Forward Information Base (FIB), a related issue to CVE-2008-2476.	2009-02-04	9.3	CVE-2009-0418 HP
hp -- 9200c_digital_sender hp -- color_laserjet_4370mfp hp -- color_laserjet_9500mfp hp -- laserjet_2410 hp -- laserjet_2420 hp -- laserjet_2430 hp -- laserjet_4250 hp -- laserjet_4345mfp hp -- laserjet_4350 hp -- laserjet_9040 hp -- laserjet_9040mfp hp -- laserjet_9050 hp -- laserjet_9050mfp	Directory traversal vulnerability in the HP JetDirect web administration interface in the HP-ChaiSOE 1.0 embedded web server on the LaserJet 9040mfp, LaserJet 9050mfp, and Color LaserJet 9500mfp before firmware 08.110.9; LaserJet 4345mfp and 9200C Digital Sender before firmware 09.120.9; Color LaserJet 4730mfp before firmware 46.200.9; LaserJet 2410, LaserJet 2420, and LaserJet 2430 before firmware 20080819 SPCL112A; LaserJet 4250 and LaserJet 4350 before firmware 20080819 SPCL015A; and LaserJet 9040 and LaserJet 9050 before firmware 20080819 SPCL110A allows remote attackers to read arbitrary files via directory traversal sequences in the URI.	2009-02-04	7.8	CVE-2008-4419 BUGTRAQ
i-rater -- i-rater_basic	SQL injection vulnerability in messages.php in I-Rater Basic allows remote attackers to execute arbitrary SQL commands via the idp parameter.	2009-02-02	7.5	CVE-2008-6017 BID MILWORM SECUNIA
ibm -- websphere_application_server	Unspecified vulnerability in IBM WebSphere Application Server (WAS) 6.0.1 on z/OS allows attackers to read arbitrary files via unknown vectors.	2009-02-02	7.8	CVE-2009-0391 BID AIXAPAR SECUNIA
	The ProcessLogin function in class.auth.php in Interspire Shopping Cart (ISC) 4.0.1			CVE-2009-0412

interspire -- shopping_cart	Ultimate edition allows remote attackers to bypass authentication and obtain administrative access by reusing the RememberToken cookie after a failed admin login attempt.	2009-02-03	7.5	V+12 XF SECTRACK BID BUGTRAQ
ircmaxell -- tech_article	SQL injection vulnerability in the Tech Articles (com_tech_article) 1.0 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the item parameter to index.php.	2009-02-04	7.5	CVE-2008-6050 BID MILWORM
jlleblanc -- com_dailymessage	SQL injection vulnerability in the Daily Message (com_dailymessage) 1.0.3 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-02-06	7.5	CVE-2008-6076 XF BID MILWORM
joomla -- com_eventing	SQL injection vulnerability in the Eventing (com_eventing) 1.6.x component for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	2009-02-04	7.5	CVE-2009-0421 XF BID MILWORM SECUNIA
kevin_walker -- php_photo_album	Directory traversal vulnerability in index.php in Php Photo Album (PHPPA) 0.8 BETA allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the preview parameter.	2009-02-04	7.5	CVE-2009-0423 XF BID MILWORM
limbo_cms -- com_privmsg	SQL injection vulnerability in open.php in the Private Messaging (com_privmsg) component for Limbo CMS allows remote attackers to execute arbitrary SQL commands via the id parameter in a pms action to index.php.	2009-02-06	7.5	CVE-2008-6078 XF BID MILWORM FRSIRT
mapcal -- mapcal	SQL injection vulnerability in index.php in MapCal 0.1 allows remote attackers to execute arbitrary SQL commands via the id parameter in an editevent action, possibly related to dsp_editevent.php.	2009-02-03	7.5	CVE-2008-6038 BID BUGTRAQ FRSIRT MISC
meet#web -- meet#web	Multiple PHP remote file inclusion vulnerabilities in Meet#Web 0.8 allow remote attackers to execute arbitrary PHP code via a URL in the root_path parameter to (1) modules.php, (2) ManagerResource.class.php, (3) ManagerRightsResource.class.php, (4) RegForm.class.php, (5) RegResource.class.php, and (6) RegRightsResource.class.php in classes/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-04	7.5	CVE-2008-6066 XF MISC BID
moxiecode -- tinymce	SQL injection vulnerability in index.php in TinyMCE 2.0.1 allows remote attackers to execute arbitrary SQL commands via the menuID parameter.	2009-02-04	7.5	CVE-2008-6049 BID MILWORM
				CVE-2009-0352

mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.6, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the layout engine and destruction of arbitrary layout objects by the nsViewManager::Composite function.	2009-02-04	CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Unspecified vulnerability in Mozilla Firefox 3.x before 3.0.6, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine.	2009-02-04	10.0 CVE-2009-0353 CONFIRM BID CONFIRM
netartmedia -- car_portal	SQL injection vulnerability in the login feature in NetArt Media Car Portal 1.0 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2009-02-02	7.5 CVE-2009-0395 BID MILWORM
netartmedia -- jobs_portal	Multiple SQL injection vulnerabilities in NetArtMedia Jobs Portal 1.3 allow remote attackers to execute arbitrary SQL commands via (1) the job parameter to index.php in the search module or (2) the news_id parameter to index.php.	2009-02-03	7.5 CVE-2008-6030 XF BID MILWORM SECUNIA
netartmedia -- real_estate_portal	SQL injection vulnerability in the re_search module in NetArtMedia Real Estate Portal 2.0 allows remote attackers to execute arbitrary SQL commands via the ad parameter to index.php.	2009-02-03	7.5 CVE-2008-6042 XF BID MILWORM
novell -- groupwise	Off-by-one error in the SMTP daemon in GroupWise Internet Agent (GWIA) in Novell GroupWise 6.5x, 7.0, 7.01, 7.02, 7.03, 7.03HP1a, and 8.0 allows remote attackers to execute arbitrary code via a long e-mail address in a malformed RCPT command, leading to a buffer overflow.	2009-02-03	10.0 CVE-2009-0410 MISC CONFIRM
php-cms_project -- php-cms_project	SQL injection vulnerability in admin/login.php in PHP-CMS Project 1 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-02-03	7.5 CVE-2009-0407 XF BID MILWORM FRSIRT
phplist -- phplist	Dynamic variable evaluation vulnerability in lists/admin.php in phpList 2.10.8 and earlier, when register_globals is disabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the _SERVER[ConfigFile] parameter to admin/index.php.	2009-02-04	7.5 CVE-2009-0422 XF BUGTRAQ MILWORM MISC SECUNIA

phpprobid -- php_pro_bid	Multiple SQL injection vulnerabilities in PHP Pro Bid (PPB) 6.04 allow remote attackers to execute arbitrary SQL commands via the (1) order_field and (2) order_type parameters to categories.php and unspecified other components. NOTE: some of these details are obtained from third party information.	2009-02-03	7.5	CVE-2008-6043 BID BUGTRAQ SECUNIA
ple_cms -- ple_cms	SQL injection vulnerability in login.php in Pre Lecture Exercises (PLEs) CMS 1.0 beta 4.2 allows remote attackers to execute arbitrary SQL commands via the school parameter.	2009-02-02	7.5	CVE-2009-0394 BID MILWORM
rasihbahar -- bahar_download_script	SQL injection vulnerability in aspkat.asp in Bahar Download Script 2.0 allows remote attackers to execute arbitrary SQL commands via the kid parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-06	7.5	CVE-2008-6075 XF BID MISC
rd-media -- rd-autos	SQL injection vulnerability in the RD-Autos (com_rdautos) 1.5.5 Stable component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-02-04	7.5	CVE-2009-0420 BID MILWORM SECUNIA
simplecustomer -- simple_customer	SQL injection vulnerability in contact.php in Simple Customer 1.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-06	7.5	CVE-2008-6081 BID MILWORM
smartsitecms -- smartsitecms	SQL injection vulnerability in articles.php in smartSite CMS 1.0 allows remote attackers to execute arbitrary SQL commands via the var parameter.	2009-02-03	7.5	CVE-2009-0405 XF BID MILWORM
sony_ericsson -- k530i sony_ericsson -- k610i sony_ericsson -- k618i sony_ericsson -- k660i sony_ericsson -- k810i sony_ericsson -- w660i sony_ericsson -- w880i sony_ericsson -- w910i sony_ericsson -- z610i	The Sony Ericsson W910i, W660i, K618i, K610i, Z610i, K810i, K660i, W880i, and K530i phones allow remote attackers to cause a denial of service (device reboot or hang-up) via a malformed WAP Push packet to (1) SMS or (2) UDP port 2948.	2009-02-02	7.8	CVE-2009-0396 SECTRACK BID BUGTRAQ MISC SECUNIA
tightvnc -- tightvnc ultravnc -- ultravnc	Multiple integer signedness errors in (1) UltraVNC 1.0.2 and 1.0.5 and (2) TightVnc 1.3.9 allow remote VNC servers to cause a denial of service (heap corruption and application crash) or possibly execute arbitrary code via a large length value in a message, related to the (a) ClientConnection::CheckBufferSize and (b) ClientConnection::CheckFileZipBufferSize functions in ClientConnection.cpp.	2009-02-04	10.0	CVE-2009-0388 BID
tor -- tor	Unspecified vulnerability in Tor before 0.2.0.33 has unspecified impact and remote attack vectors that trigger heap corruption.	2009-02-03	10.0	CVE-2009-0414 BID CONFIRM
	Directory traversal vulnerability in			

txtshop -- txtshop	header.php in TXTshop beta 1.0 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the language parameter.	2009-02-06	7.5	CVE-2008-6083 MILWORM
university_of_queensland -- fez	SQL injection vulnerability in list.php in University of Queensland Library Fez 1.3 and 2.0 RC1 allows remote attackers to execute arbitrary SQL commands via the parent_id parameter in a subject action.	2009-02-03	7.5	CVE-2008-6028 BID MILWORM FRSIRT
wsn -- links	SQL injection vulnerability in comments.php in WSN Links Free 4.0.34P allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-03	7.5	CVE-2008-6032 MILWORM FRSIRT
wsn_links -- wsn_links	SQL injection vulnerability in vote.php in WSN Links 2.22 and 2.23 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-03	7.5	CVE-2008-6031 BID MILWORM
wsn_links -- wsn_links	SQL injection vulnerability in comments.php in WSN Links 2.20 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-03	7.5	CVE-2008-6033 BID MILWORM
xnova -- xnova	PHP remote file inclusion vulnerability in includes/todofleetcontrol.php in an older version of Xnova, possibly 0.8 sp1, allows remote attackers to execute arbitrary PHP code via a URL in the ugamelia_root_path parameter.	2009-02-02	7.5	CVE-2008-6022 BID MILWORM
xnova -- xnova	PHP remote file inclusion vulnerability in includes/todofleetcontrol.php in a newer version of Xnova, possibly 0.8 sp1, allows remote attackers to execute arbitrary PHP code via a URL in the xnova_root_path parameter.	2009-02-02	7.5	CVE-2008-6023 BID MILWORM

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

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
.matteoiammarrone -- iamma_simple_gallery	Unrestricted file upload vulnerability in pages/download.php in Iamma Simple Gallery 1.0 and 2.0 allows remote attackers to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a direct request to the file in the uploads directory .	2009-02-06	6.8	CVE-2008-6084 BID MILWORM SECUNIA
achieveo -- achieveo	Cross-site scripting (XSS) vulnerability in dispatch.php in Achievo 1.3.2 allows remote attackers to inject arbitrary web script or HTML via the atkaction parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-03	4.3	CVE-2008-6034 BID SECUNIA
achieveo -- achieveo	Cross-site scripting (XSS) vulnerability in dispatch.php in Achievo 1.3.2-STABLE allows remote attackers to inject arbitrary	2009-02-02	4.3	CVE-2008-6035 BID

	web script or HTML via the atknodetype parameter.	v3	BID MISC
activewebsoftwares -- active_bids	Multiple cross-site scripting (XSS) vulnerabilities in Active Bids allow remote attackers to inject arbitrary web script or HTML via the (1) search parameter to search.asp and the (2) URL parameter to tellafriend.asp.	2009-02-04	4.3 CVE-2009-0430 BID BUGTRAQ
adbnewssender -- adbnewssender	Cross-site scripting (XSS) vulnerability in ADbNewsSender before 1.5.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to (1) subscribing and (2) unsubscribing.	2009-02-04	4.3 CVE-2008-6047 BID CONFIRM SECUNIA
adobe -- dreamweaver	Cross-site scripting (XSS) vulnerability in ActionScript in arbitrary Shockwave Flash (SWF) files created by Adobe Dreamweaver, when the Insert Flash Video feature is used, allows remote attackers to inject arbitrary web script or HTML via an asfunction: URI in the skinName parameter. NOTE: this may overlap CVE-2007-6242, CVE-2007-6244, or CVE-2007-6637.	2009-02-04	4.3 CVE-2008-6062 CERT-VN
an_guestbook -- an_guestbook	Cross-site scripting (XSS) vulnerability in sign1.php in AN Guestbook (ANG) before 0.7.7 allows remote attackers to inject arbitrary web script or HTML via the country parameter, which is not properly handled in (1) administrator/manage.php or (2) administrator/trash.php. NOTE: some of these details are obtained from third party information.	2009-02-04	4.3 CVE-2009-0424 BID
bioinformatics -- htmlawed	Multiple cross-site scripting (XSS) vulnerabilities in Bioinformatics htmLawed 1.1.3 and 1.1.4 allow remote attackers to inject arbitrary web script or HTML via invalid Cascading Style Sheets (CSS) expressions in the style attribute, which is processed by Internet Explorer 7.	2009-02-03	4.3 CVE-2009-0404 BID CONFIRM CONFIRM SECUNIA CONFIRM
bluepage -- bluepage_cms	Multiple cross-site scripting (XSS) vulnerabilities in index.php in BLUEPAGE CMS 2.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) whl, (2) var_1, and (3) search parameters.	2009-02-03	4.3 CVE-2008-6027 BID BUGTRAQ MISC
bluepage -- bluepage_cms	Session fixation vulnerability in BLUEPAGE CMS 2.5 and earlier allows remote attackers to hijack web sessions by setting the PHPSESSID parameter.	2009-02-03	6.8 CVE-2008-6039 BID BUGTRAQ MISC
buzzywall -- buzzywall	SQL injection vulnerability in search.php in BuzzyWall 1.3.1 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the search parameter.	2009-02-03	6.8 CVE-2008-6029 BID MILWORM
cisco -- 4400_wireless_lan_controller cisco --	The Cisco Wireless LAN Controller (WLC), Cisco Catalyst 6500 Wireless Services Module (WiSM), and Cisco Catalyst 3750		

catalyst_3750_series_integrated_wireless_lan_controller cisco -- catalyst_6500_series_integrated_wireless_lan_controller cisco -- catalyst_7600_series_wireless_lan_controller cisco -- wireless_lan_controller	Integrated Wireless LAN Controller with software 4.x before 4.2.176.0 and 5.x before 5.2 allow remote attackers to cause a denial of service (web authentication outage or device reload) via unspecified network traffic, as demonstrated by a vulnerability scanner.	2009-02-04	6.1	CVE-2009-0058 CISCO
codecall -- com_ionfiles	Directory traversal vulnerability in download.php in the ionFiles (com_ionfiles) 4.4.2 component for Joomla! allows remote attackers to read arbitrary files via a ..(dot dot) in the file parameter.	2009-02-06	5.0	CVE-2008-6080 XF BID MILWORM SECUNIA
dataspade -- dataspade	Multiple cross-site scripting (XSS) vulnerabilities in Index.asp in Dataspade 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) ViewName, (2) TableName, (3) OrderBy, and (4) FilterField parameters.	2009-02-03	4.3	CVE-2008-6041 BID SECUNIA MISC
domphp -- domphp	Multiple SQL injection vulnerabilities in DomPHP 0.81 allow remote attackers to execute arbitrary SQL commands via the cat parameter to agenda/index.php, and unspecified other vectors.	2009-02-04	6.8	CVE-2008-6064 BID MILWORM
enomaly -- elastic_computing_platform	Enomaly Elastic Computing Platform (ECP), formerly Enomalism, before 2.1.1 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/enomalism2.pid temporary file.	2009-02-02	6.9	CVE-2008-4990 BUGTRAQ
ex-designs -- world_recipe	Multiple cross-site scripting (XSS) vulnerabilities in World Recipe 2.11 allow remote attackers to inject arbitrary web script or HTML via the (1) n parameter to emailrecipe.aspx, (2) id parameter to recipedetail.aspx, and the (3) catid parameter to validatefieldlength.aspx.	2009-02-04	4.3	CVE-2008-6056 XF BID BUGTRAQ
goahead -- goahead_webserver	The security handler in GoAhead WebServer before 2.1.1 allows remote attackers to bypass authentication and obtain access to protected web content via "an extra slash in a URL," a different vulnerability than CVE-2002-1603.	2009-02-06	5.0	CVE-2002-2427 CERT-VN CONFIRM
goahead -- goahead_webserver	webs.c in GoAhead WebServer before 2.1.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an HTTP POST request that contains a Content-Length header but no body data.	2009-02-06	5.0	CVE-2002-2428 CONFIRM
goahead -- goahead_webserver	webs.c in GoAhead WebServer before 2.1.4 allows remote attackers to cause a denial of service (daemon crash) via an HTTP POST request that contains a negative integer in the Content-Length header.	2009-02-06	5.0	CVE-2002-2429 CONFIRM
goahead -- goahead_webserver	GoAhead WebServer before 2.1.1 allows remote attackers to cause a denial of service (CPU consumption) by performing a socket disconnect to terminate a request before it has been fully processed by the server.	2009-02-06	5.0	CVE-2002-2430 CONFIRM

google -- chrome	Cross-domain vulnerability in the V8 JavaScript engine in Google Chrome before 1.0.154.46 allows remote attackers to bypass the Same Origin Policy via a crafted script that accesses another frame and reads its full URL and possibly other sensitive information, or modifies the URL of this frame.	2009-02-03	5.0	CVE-2009-0276 CONFIRM CONFIRM SECUNIA CONFIRM CONFIRM
google -- chrome	Google Chrome before 1.0.154.46 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls and other web script.	2009-02-03	5.0	CVE-2009-0411 CONFIRM CONFIRM CONFIRM CONFIRM
infosoftglobal -- fusion_charts	Cross-site scripting (XSS) vulnerability in ActionScript in arbitrary Shockwave Flash (SWF) files created by InfoSoft FusionCharts allows remote attackers to inject arbitrary additional SWF content via a URL in the SRC attribute of an IMG element in the dataURL parameter.	2009-02-04	4.3	CVE-2008-6060 CERT-VN BUGTRAQ FRSIRT MISC
liberum -- liberum_help_desk	Doug Luxem Liberum Help Desk 0.97.3 stores db/helpdesk2000.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request.	2009-02-04	5.0	CVE-2008-6057 XF MILWORM
loudblog -- loudblog	SQL injection vulnerability in loudblog/ajax.php in LoudBlog 0.8.0a and earlier allows remote authenticated users to execute arbitrary SQL commands via the colpick parameter in a singleread action.	2009-02-06	6.5	CVE-2008-6077 BID MILWORM SECUNIA
metalinks -- metacart	MetaCart Free stores metacart.mdb under the web root with insufficient access control, which allows remote attackers to obtain usernames and passwords via a direct request.	2009-02-04	5.0	CVE-2008-6051 BUGTRAQ
microsoft -- xml_core_services	Microsoft XML Core Services, as used in Microsoft Expression Web, Office, Internet Explorer 6 and 7, and other products, does not properly restrict access from web pages to Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls, related to the HTTPOnly protection mechanism. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-4033.	2009-02-04	5.0	CVE-2009-0419 MISC
microsoft -- word	Microsoft Word 2007, when the "Save as PDF" add-on is enabled, places an absolute pathname in the Subject field during an "Email as PDF" operation, which allows remote attackers to obtain sensitive information such as the sender's account name and a Temporary Internet Files subdirectory name.	2009-02-04	4.3	CVE-2008-6063 BUGTRAQ
	Directory traversal vulnerability in sysconf.cgi in Motorola Wimax modem	2009-02-03		CVE-2009-0392

motorola -- cpei300	CPEi300 allows remote authenticated users to read arbitrary files via a .. (dot dot) in the page parameter.	2009-02-02	6.8	BID BUGTRAQ MILWORM
mozilla -- firefox	components/sessionstore/src/nsSessionStore.js in Mozilla Firefox before 3.0.6 does not block changes of INPUT elements to type="file" during tab restoration, which allows user-assisted remote attackers to read arbitrary files on a client machine via a crafted INPUT element.	2009-02-04	5.4	CVE-2009-0355 CONFIRM BID CONFIRM
mozilla -- firefox	Mozilla Firefox before 3.0.6 and SeaMonkey do not block links to the (1) about:plugins and (2) about:config URIs from .desktop files, which allows user-assisted remote attackers to bypass the Same Origin Policy and execute arbitrary code with chrome privileges via vectors involving the URL field in a Desktop Entry section of a .desktop file, related to representation of about: URIs as jar:file:/// URIs. NOTE: this issue exists because of an incomplete fix for CVE-2008-4582.	2009-02-04	5.1	CVE-2009-0356 CONFIRM BID CONFIRM
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.6 and SeaMonkey before 1.1.15 do not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls, related to the HTTPOnly protection mechanism.	2009-02-04	5.0	CVE-2009-0357 CONFIRM BID CONFIRM MISC
myphpsite -- myphpsite	Directory traversal vulnerability in index.php in MyPHPSite, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the mod parameter.	2009-02-02	6.8	CVE-2008-6018 BID MILWORM SECUNIA
mzbservices -- max.blog	SQL injection vulnerability in offline_auth.php in Max.Blog 1.0.6 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-02-03	6.8	CVE-2009-0409 BID BUGTRAQ MILWORM SECUNIA
novell -- groupwise	Cross-site request forgery (CSRF) vulnerability in Novell GroupWise WebAccess 6.5x, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 allows remote attackers to insert e-mail forwarding rules, and modify unspecified other configuration settings, as arbitrary users via unknown vectors.	2009-02-02	6.8	CVE-2009-0272 BUGTRAQ MISC CONFIRM SECUNIA
novell -- groupwise	Multiple cross-site scripting (XSS) vulnerabilities in Novell GroupWise WebAccess 6.5x, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 allow remote attackers to inject arbitrary web script or HTML via the (1) User.id and (2) Library.queryText parameters to gw/webacc, and other vectors involving (3) HTML e-mail and (4) HTML	2009-02-02	4.3	CVE-2009-0273 BID BID BUGTRAQ BUGTRAQ MISC MISC CONFIRM

	attachments.		CONFIRM SECUNIA
novell -- groupwise	Unspecified vulnerability in WebAccess in Novell GroupWise 6.5, 7.0, 7.01, 7.02x, 7.03, 7.03HP1a, and 8.0 might allow remote attackers to obtain sensitive information via a crafted URL, related to conversion of POST requests to GET requests.	2009-02-03	5.0 CVE-2009-0274 BID CONFIRM SECUNIA
openelec -- openelec	Directory traversal vulnerability in scr/form.php in openElec 3.01 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the obj parameter.	2009-02-03	6.8 CVE-2008-6025 XF BID MILWORM
oracle -- database_server	Oracle Database Server 10.1, 10.2, and 11g grants directory WRITE permissions for arbitrary pathnames that are aliased in a CREATE OR REPLACE DIRECTORY statement, which allows remote authenticated users with CREATE ANY DIRECTORY privileges to gain SYSDBA privileges by aliasing the pathname of the password directory, and then overwriting the password file through UTL_FILE operations, a related issue to CVE-2006-7141.	2009-02-04	5.1 CVE-2008-6065 BID BUGTRAQ MISC
oscommerce -- oscommerce	Cross-site request forgery (CSRF) vulnerability in osCommerce 2.2 RC 2a allows remote attackers to perform unauthorized actions as administrators via unspecified vectors.	2009-02-03	6.0 CVE-2009-0408 XF SECUNIA OSVDB
phpcrs -- phpcrs	Directory traversal vulnerability in frame.php in phpcrs 2.06 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the importFunction parameter.	2009-02-06	5.1 CVE-2008-6074 BID MILWORM SECUNIA
preprojects -- pre_e-learning_portal	PreProjects Pre E-Learning Portal stores db_elearning.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request.	2009-02-04	5.0 CVE-2008-6052 SECUNIA MISC
preprojects -- pre_resume_submitter	PreProjects Pre Resume Submitter stores onlinerresume.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request.	2009-02-04	5.0 CVE-2008-6053 SECUNIA MISC
preprojects -- pre_classified_listings	PreProjects Pre Classified Listings stores pclasp.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request.	2009-02-04	5.0 CVE-2008-6055 SECUNIA MISC
preprojects.com -- pre_courier_and_cargo_business	PreProjects Pre Courier and Cargo Business stores dbcourior.mdb under the web root with insufficient access control, which allows remote attackers to obtain passwords via a direct request.	2009-02-04	5.0 CVE-2008-6054 SECUNIA MISC
	The verifyProof function in the Token		

redhat -- _dogtag_certificate_system redhat -- certificate_system	Processing System (TPS) component in Red Hat Certificate System (RHCS) 7.1 through 7.3 and Dogtag Certificate System 1.0 returns successfully even when token enrollment did not use the hardware key, which allows remote authenticated users with enrollment privileges to bypass intended authentication policies by performing enrollment with a software key.	2009-01-30	6.0	CVE-2008-5082 REDHAT CONFIRM XF BID FRSIRT SECUNIA
roundcube -- roundcube_webmail	Cross-site scripting (XSS) vulnerability in RoundCube Webmail (roundcubemail) 0.2 stable allows remote attackers to inject arbitrary web script or HTML via the background attribute embedded in an HTML e-mail message.	2009-02-03	4.3	CVE-2009-0413 XF BID CONFIRM SECUNIA
socialengine -- socialengine	SQL injection vulnerability in blog.php in SocialEngine 3.06 trial allows remote attackers to execute arbitrary SQL commands via the category_id parameter.	2009-02-03	6.8	CVE-2009-0400 XF BID MILWORM SECUNIA
southrivertech -- titan_ftp_server	Titan FTP Server 6.26 build 630 allows remote attackers to cause a denial of service (CPU consumption) via the SITE WHO command.	2009-02-06	5.0	CVE-2008-6082 BID OSVDB MILWORM SECUNIA
standards_based_linux_instrumentation -- sblim-sfcb	The SSL certificate setup program (genSslCert.sh) in Standards Based Linux Instrumentation for Manageability (SBLIM) sblim-sfcb 1.3.2 allows local users to overwrite arbitrary files via a symlink attack on the (1) /var/tmp/key.pem, (2) /var/tmp/cert.pem, and (3) /var/tmp/ssl.cnf temporary files.	2009-02-03	6.9	CVE-2009-0416 BID MISC MLIST
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the NFSv4 client module in the kernel on Sun Solaris 10 and OpenSolaris before snv_37, when automountd is used, allows user-assisted remote attackers to cause a denial of service (unresponsive NFS filesystems) via unknown vectors.	2009-02-02	5.4	CVE-2008-6024 SUNALERT
syslserve -- syslserve	Syslserve 1.058 and earlier, and probably 1.059, allows remote attackers to cause a denial of service (hang) via a crafted UDP Syslog packet.	2009-02-04	5.0	CVE-2008-6058 CONFIRM BID MISC SECUNIA
tangocms -- tangocms	Multiple cross-site request forgery (CSRF) vulnerabilities in TangoCMS before 2.2.0 allow remote attackers to perform unauthorized actions as administrators via unspecified vectors.	2009-02-04	6.0	CVE-2008-6048 CONFIRM SECUNIA OSVDB
	Cross-site scripting (XSS) vulnerability in ActionScript in arbitrary Shockwave Flash (SWF) controller files created by Techsmith	2009-02-04		CVE-2008-6061 CERT-VN

techsmith -- camtasia_studio	Camtasia Studio before 5 allows remote attackers to inject arbitrary additional SWF content via a URL in the csPreloader parameter.	2009-02-04	4.3	BUGTRAQ FRSIRT SECUNIA MISC
vmware -- esx vmware -- esxi	Unspecified vulnerability in VMware ESXi 3.5 before ESXe350-200901401-I-SG and ESX 3.5 before ESX350-200901401-SG allows local administrators to cause a denial of service (host crash) via a snapshot with a malformed VMDK delta disk.	2009-02-03	4.7	CVE-2008-4914 BID
webkit -- webkit	xml/XMLHttpRequest.cpp in WebCore in WebKit before r38566 does not properly restrict access from web pages to the (1) Set-Cookie and (2) Set-Cookie2 HTTP response headers, which allows remote attackers to obtain sensitive information from cookies via XMLHttpRequest calls, related to the HTTPOnly protection mechanism.	2009-02-04	5.0	CVE-2008-6059 CONFIRM CONFIRM
xt-commerce -- xt-commerce	Cross-site scripting (XSS) vulnerability in advanced_search_result.php in xt:Commerce 3.0.4 and earlier allows remote attackers to inject arbitrary web script or HTML via the keywords parameter.	2009-02-03	4.3	CVE-2008-6044 BID BUGTRAQ MISC
xt-commerce -- xt-commerce	Session fixation vulnerability in xt:Commerce 3.0.4 and earlier allows remote attackers to hijack web sessions by setting the XTCsid parameter.	2009-02-03	6.8	CVE-2008-6045 BID BUGTRAQ BUGTRAQ MISC

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

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
monkey -- trickle	Untrusted search path vulnerability in trickle 1.07 allows local users to execute arbitrary code via a Trojan horse trickle-overload.so in the current working directory, which is referenced in the LD_PRELOAD path.	2009-02-03	3.7	CVE-2009-0415 BID MLIST MISC
motorola -- cpei300	Cross-site scripting (XSS) vulnerability in sysconf.cgi in Motorola Wimax modem CPEi300 allows remote authenticated users to inject arbitrary web script or HTML via the page parameter.	2009-02-02	3.5	CVE-2009-0393 BID BUGTRAQ MILWORM
mozilla -- firefox	Cross-domain vulnerability in js/src/jsobj.cpp in Mozilla Firefox 3.x before 3.0.6 allows remote attackers to bypass the Same Origin Policy, and access the properties of an arbitrary window and conduct cross-site scripting (XSS) attacks, via vectors involving a chrome XBL method and the window.eval function.	2009-02-04	2.6	CVE-2009-0354 CONFIRM BID CONFIRM
mozilla -- firefox	Mozilla Firefox 3.x before 3.0.6 does not properly implement the (1) no-store and (2) no-cache Cache-Control directives, which allows local users to obtain sensitive information by using the (a) back button or (b) history list of the victim's	2009-02-04	3.3	CVE-2009-0358 CONFIRM BID CONFIRM

browser, as demonstrated by reading the response page of an https POST request.

[CONTINUE](#)
[MISC](#)

[Back to top](#)