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**
4site -- 4site_cms	Multiple SQL injection vulnerabilities in 4Site CMS 2.6 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) login and (2) password parameters to pcgi/4site.pl, (3) page parameter to print/print.shtml, (4) s and (5) i parameters to portfolio/index.shtml, (6) h parameter to hotel/index.php, (7) id parameter to news/news1.shtml, and the (8) th parameter to faq/index.shtml.	2009-02-18	7.5	CVE-2009-0646 XF XF XF XF BID OSVDB OSVDB OSVDB OSVDB MILW0RM MISC SECUNIA
android -- android_sdk	Integer overflow in the showLog function in fake_log_device.c in liblog in Open Handset Alliance Android 1.0 allows attackers to trigger a buffer overflow and possibly have unspecified other impact by sending a large number of input lines.	2009-02-17	7.2	CVE-2009-0608 BID BUGTRAQ
barnowel -- barnowel barnowel -- owel	Multiple buffer overflows in (a) BarnOwl before 1.0.5 and (b) owl 2.1.11 allow remote attackers to execute arbitrary code via vectors involving (1) a crafted zcrypt message, related to zcrypt.c; (2) a reply command on a message with a Zephyr Cc: list, related to zwrite.c; and unspecified other use of the products.	2009-02-17	7.5	CVE-2009-0363 CONFIRM MLIST CONFIRM CONFIRM CONFIRM
bookingcentre -- booking_system_for_hotels_group	SQL injection vulnerability in cadena_ofertas_ext.php in Venalsur Booking center Booking System for Hotels Group allows remote attackers to execute arbitrary SQL commands via the OfertaID parameter.	2009-02-20	7.5	CVE-2008-6216 MILW0RM

bux -- bux.to_clone_script	Bux.to Clone script allows remote attackers to bypass authentication and gain administrative access by setting the loggedin cookie to 1 and the usNick cookie to admin.	2009-02-20	7.5	CVE-2008-6162 BID MILW0RM
dminnich -- simple_php_news	Multiple static code injection vulnerabilities in post.php in Simple PHP News 1.0 final allow remote attackers to inject arbitrary PHP code into news.txt via the (1) title or (2) date parameter, and then execute the code via a direct request to display.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-17	7.5	CVE-2009-0610 SECUNIA OSVDB
dream4 -- koobi	SQL injection vulnerability in index.php in dream4 Koobi 4.4 and 5.4 allows remote attackers to execute arbitrary SQL commands via the img_id parameter in the gallerypic page.	2009-02-19	7.5	CVE-2008-6210 XF BID MILW0RM MISC
drupal -- everyblog	Unspecified vulnerability in EveryBlog 5.x and 6.x, a module for Drupal, allows remote attackers to gain privileges as another user or an administrator via unknown attack vectors.	2009-02-13	7.5	CVE-2008-6136 BID SECUNIA CONFIRM
drupal -- drupal	Drupal 5.x before 5.12 and 6.x before 6.6, when the server is configured for "IP-based virtual hosts," allows remote attackers to include and execute arbitrary files via unspecified vectors.	2009-02-19	9.3	CVE-2008-6171 BID CONFIRM
drupal -- drupal	bootstrap.inc in Drupal 5.x before 5.12 and 6.x before 6.6, when the server is configured for "IP-based virtual hosts," allows remote attackers to include and execute arbitrary local files via unspecified vectors.	2009-02-19	7.5	CVE-2008-6176 BID CONFIRM
falt4 -- falt4_cms tru-zone -- nukeet	Unrestricted file upload vulnerability in editor/filemanager/browser/default/connectors/php/connector.php in FCKeditor 2.2, as used in Falt4 CMS, Nuke ET, and other products, allows remote attackers to execute arbitrary code by creating a file with PHP sequences preceded by a ZIP header, uploading this file via a FileUpload action with the application/zip content type, and then accessing this file via a direct request to the file in UserFiles/File/, probably a related issue to CVE-2005-4094. NOTE: some of these details are obtained from third party information.	2009-02-19	7.5	CVE-2008-6178 XF BID MILW0RM FRSIRT SECUNIA
fivedollarscripts -- drinks	SQL injection vulnerability in index.php in Five Dollar Scripts Drinks script allows remote attackers to execute arbitrary SQL commands via the recid parameter.	2009-02-20	7.5	CVE-2008-6233 BID MILW0RM FRSIRT SECUNIA
freebsd -- freebsd	sys_term.c in telnetd in FreeBSD 7.0-RELEASE and other 7.x versions deletes dangerous environment variables with a method that was valid only in older FreeBSD distributions, which might allow remote attackers to execute arbitrary code by passing a crafted environment variable from a telnet client, as demonstrated by an LD_PRELOAD value that references a malicious library.	2009-02-20	9.3	CVE-2009-0641 FREEBSD
				CVE-2008-6187

gforge -- gforge	SQL injection vulnerability in frs/shownotes.php in Gforge 4.5.19 and earlier allows remote attackers to execute arbitrary SQL commands via the release_id parameter.	2009-02-19	7.5	XF BID SECUNIA MILW0RM CONFIRM
gforge -- gforge	SQL injection vulnerability in people/editprofile.php in Gforge 4.6 rc1 and earlier allows remote attackers to execute arbitrary SQL commands via the skill_edit[] parameter.	2009-02-19	7.5	CVE-2008-6188 BID SECUNIA MILW0RM CONFIRM
gforge -- gforge	SQL injection vulnerability in GForge 4.5.19 allows remote attackers to execute arbitrary SQL commands via the offset parameter to (1) new/index.php, (2) news/index.php and (3) top/topusers.php, which is not properly handled in database-pgsql.php.	2009-02-19	7.5	CVE-2008-6189 XF SECUNIA CONFIRM
harlandscripts -- pro_traffic_one	SQL injection vulnerability in mypage.php in Harlandscripts Pro Traffic One allows remote attackers to execute arbitrary SQL commands via the trg parameter.	2009-02-20	7.5	CVE-2008-6213 BID BUGTRAQ MILW0RM SECUNIA
harlandscripts -- pro_traffic_one	SQL injection vulnerability in poll_results.php in Harlandscripts Pro Traffic One allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-20	7.5	CVE-2008-6214 MILW0RM SECUNIA
hispah -- text_links_ads	SQL injection vulnerability in index.php in Hispah Text Links Ads 1.1 allows remote attackers to execute arbitrary SQL commands via the idcat parameter.	2009-02-16	7.5	CVE-2008-6154 BID MILW0RM SECUNIA
hispah -- text_links_ads	SQL injection vulnerability in index.php in Hispah Text Links Ads 1.1 allows remote attackers to execute arbitrary SQL commands via the idtl parameter in a buy action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-16	7.5	CVE-2008-6155 SECUNIA
indexscript -- indexscript	SQL injection vulnerability in sug_cat.php in IndexScript 3.0 allows remote attackers to execute arbitrary SQL commands via the parent_id parameter, a different vector than CVE-2007-4069.	2009-02-19	7.5	CVE-2008-6179 BID MILW0RM SECUNIA
jakob-persson -- cobalt	SQL injection vulnerability in CoBaLT 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter to (1) urun.asp, (2) admin/bayi_listele.asp, (3) admin/urun_grup_listele.asp, and (4) admin/urun_listele.asp.	2009-02-19	7.5	CVE-2008-6202 MILW0RM
jakob-persson -- cobalt	SQL injection vulnerability in adminler.asp in CoBaLT 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	7.5	CVE-2008-6203 XF MISC BID
jayeshp -- pixel8_web_photo_album	SQL injection vulnerability in Photo.asp in Jay Patel Pixel8 Web Photo Album 3.0 allows remote attackers to execute arbitrary SQL commands via the AlbumID parameter	2009-02-16	7.5	CVE-2008-6153 XF BID

	SQL commands via the AboutID parameter.			MILW0RM SECUNIA
joomla -- com_kbase	SQL injection vulnerability in the KBase (com_kbase) 1.2 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in an article action to index.php.	2009-02-18	7.5	CVE-2008-6166 BID MILW0RM
joomla -- ignitegallery	SQL injection vulnerability in the Ignite Gallery (com_ignitegallery) component 0.8.0 through 0.8.3 for Joomla! allows remote attackers to execute arbitrary SQL commands via the gallery parameter in a view action to index.php.	2009-02-19	7.5	CVE-2008-6182 XF BID MILW0RM SECUNIA
joomla -- ownbiblio	SQL injection vulnerability in the OwnBiblio (com_ownbiblio) component 1.5.3 for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter in a catalogue action to index.php.	2009-02-19	7.5	CVE-2008-6184 XF BID MILW0RM SECUNIA
kwsphp -- galerie_module	SQL injection vulnerability in index.php in the galerie module for KwsPHP 1.3.456 allows remote attackers to execute arbitrary SQL commands via the id_gal parameter in a gal action.	2009-02-19	7.5	CVE-2008-6197 XF BID MILW0RM
landesk -- landesk_management_suite	Directory traversal vulnerability in the PXE TFTP Service (PXEMTFTP.exe) in LANDesk Management Suite (LDMS) 8.80.1.1 and earlier allows remote attackers to read arbitrary files via a subdirectory name followed by ".." sequences, a different vulnerability than CVE-2008-1643.	2009-02-19	7.8	CVE-2008-6195 CONFIRM
mad4media -- com_mad4joomla	SQL injection vulnerability in the Mad4Joomla Mailforms (com_mad4joomla) component before 1.1.8.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the jid parameter to index.php.	2009-02-19	7.5	CVE-2008-6181 XF BID MILW0RM CONFIRM CONFIRM SECUNIA
microsoft -- windows	Memory leak in the DNS server in Microsoft Windows allows remote attackers to cause a denial of service (memory consumption) via DNS packets. NOTE: this issue reportedly exists because of an incorrect fix for CVE-2007-3898.	2009-02-19	7.8	CVE-2008-6194 BUGTRAQ BUGTRAQ
miniportail -- miniportail	Directory traversal vulnerability in search.php in miniPortail 2.2 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lng parameter.	2009-02-19	7.5	CVE-2008-6167 BID MILW0RM
mole-group -- airline_ticket_sale_script	** DISPUTED ** SQL injection vulnerability in info.php in Mole Group Airline Ticket Sale Script allows remote attackers to execute arbitrary SQL commands via the flight parameter. NOTE: the vendor has disputed this issue, stating "crazy hackers and so named Security companies [spread] out such false informations. Such scripts or versions [do not] exist."	2009-02-20	7.5	CVE-2008-6225 MISC MILW0RM FRSIRT SECUNIA
mybboard -- custom_pages_plugin	SQL injection vulnerability in pages.php in Custom Pages 1.0 plugin for MyBulletinBoard (MyBB) allows remote attackers to execute arbitrary SQL commands via the page parameter.	2009-02-19	7.5	CVE-2008-6198 XF BID

				MILW0RM
myphpindexer -- my_php_indexer	Multiple directory traversal vulnerabilities in index.php in My PHP Indexer 1.0 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) d and (2) f parameters.	2009-02-19	7.8	CVE-2008-6183 XF BID MILW0RM FRSIRT SECUNIA
newlife_blogger -- newlife_blogger	SQL injection vulnerability in system/nlb_user.class.php in NewLife Blogger 3.0 and earlier, and possibly 3.3.1, allows remote attackers to execute arbitrary SQL commands via the nlb3 cookie.	2009-02-19	7.5	CVE-2008-6180 XF XF BID BUGTRAQ MISC MILW0RM FRSIRT SECUNIA
novell -- opensuse opensuse -- opensuse	Buffer overflow in SUSE blinux (aka sbl) in SUSE openSUSE 10.3 through 11.0 has unknown impact and attack vectors related to "incoming data and authentication-strings."	2009-02-18	7.2	CVE-2009-0310 BID SUSE
openhandsetalliance -- android_sdk	The link_image function in linker/linker.c in the dynamic linker in Bionic in Open Handset Alliance Android 1.0 on the T-Mobile G1 phone does not properly handle file descriptors 0, 1, and 2 for a setgid program, which allows local users to create arbitrary files owned by certain groups, possibly a related issue to CVE-2002-0820.	2009-02-17	7.2	CVE-2009-0606 BID BUGTRAQ
openhandsetalliance -- android_sdk	Multiple integer overflows in malloc_leak.c in Bionic in Open Handset Alliance Android 1.0 have unknown impact and attack vectors, related to the (1) chk_calloc and (2) leak_calloc functions.	2009-02-17	7.2	CVE-2009-0607 BID BUGTRAQ
openx -- openx	SQL injection vulnerability in www/delivery/ac.php in OpenX 2.6.1 allows remote attackers to execute arbitrary SQL commands via the bannerid parameter.	2009-02-20	7.5	CVE-2008-6163 BID
philippe_crochat -- easysite	Multiple PHP remote file inclusion vulnerabilities in Philippe CROCHAT EasySite 2.0 allow remote attackers to execute arbitrary PHP code via a URL in the EASYSITE_BASE parameter to (1) browser.php, (2) image_editor.php and (3) skin_chooser.php in configuration/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	7.5	CVE-2008-6196 XF MISC BID
php_director -- php_director	SQL injection vulnerability in index.php in PHP Director 0.21 and earlier allows remote attackers to execute arbitrary SQL commands via the searching parameter.	2009-02-16	7.5	CVE-2009-0604 BID MILW0RM FRSIRT
phpg_upload -- phpg_upload	Unrestricted file upload vulnerability in form_upload.php in PHPG Upload 1.0 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	8.5	CVE-2008-6207 XF BID
				CVE-2009-

phpmesfilms -- phpmesfilms	SQL injection vulnerability in index.php in PhpMesFilms 1.0 and 1.8 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-16	7.5	0598 BID MILW0RM SECUNIA
phpyabs -- phpyabs	PHP remote file inclusion vulnerability in moduli/libri/index.php in phpyabs 0.1.2 allows remote attackers to execute arbitrary PHP code via a URL in the Azione parameter.	2009-02-18	7.5	CVE-2009-0639 BID MILW0RM
pnphpbb -- pnphpbb2	Multiple directory traversal vulnerabilities in PNphpBB2 1.2i and earlier allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the ModName parameter to (1) admin_words.php, (2) admin_groups_reapir.php, (3) admin_smilies.php, (4) admin_ranks.php, (5) admin_styles.php, and (6) admin_users.php in admin/.	2009-02-16	7.5	CVE-2009-0592 BID MILW0RM SECUNIA
preproject -- pre_podcast_portal	SQL injection vulnerability in Tour.php in Pre Projects Pre Podcast Portal allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-20	7.5	CVE-2008-6230 BID MILW0RM FRSIRT SECUNIA
raidenftpd -- raidenftpd	Stack-based buffer overflow in RaidenFTPD 2.4 build 3620 allows remote authenticated users to cause a denial of service (crash) or execute arbitrary code via long (1) CWD and (2) MLST commands.	2009-02-19	9.0	CVE-2008-6186 BID MILW0RM FRSIRT SECUNIA
robotstats -- robotstats	Multiple PHP remote file inclusion vulnerabilities in RobotStats 0.1 allow remote attackers to execute arbitrary PHP code via a URL in the DOCUMENT_ROOT parameter to (1) graph.php and (2) robotstats.inc.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	7.5	CVE-2008-6206 XF MISC BID
sepcity -- classified_ads	SQL injection vulnerability in classdis.asp in SepCity Classified Ads allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2009-02-16	7.5	CVE-2008-6150 XF BID SECUNIA MILW0RM
sepcity -- shopping_mall	SQL injection vulnerability in shpdetails.asp in SepCity Shopping Mall allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2009-02-16	7.5	CVE-2008-6151 XF BID MILW0RM SECUNIA
sepcity -- faculty_portal	SQL injection vulnerability in deptdisplay.asp in SepCity Faculty Portal allows remote attackers to execute arbitrary SQL commands via the ID parameter. NOTE: this was originally reported for Lawyer Portal, which does not have a deptdisplay.asp file.	2009-02-16	7.5	CVE-2008-6152 XF BID MILW0RM SECUNIA
sun -- java_system_directory_server	Sun Java System Directory Proxy Server in Sun Java System Directory Server Enterprise Edition 6.0 through 6.3, when a JDBC data source is used, does not properly handle (1) a long value in an ADD or (2) long string attributes, which allows remote attackers to cause a denial of service (JDBC backend	2009-02-17	7.8	CVE-2009-0609 SUNALERT CONFIRM

	outage) via crafted LDAP requests.			
supernet -- supernet_shop	Multiple SQL injection vulnerabilities in SuperNET Shop 1.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to secure/admin/guncelle.asp, (2) kulad and sifre parameters to secure/admin/giris.asp, and (3) username and password to secure/admin/default.asp.	2009-02-19	7.5	CVE-2008-6204 XF BID MILW0RM FRSIRT
vastal -- software_zone	SQL injection vulnerability in view_product.php in Vastal I-Tech Software Zone allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2009-02-19	7.5	CVE-2008-6209 XF BID MILW0RM MILW0RM
w3bcms -- w3b>cms	Multiple unspecified vulnerabilities in the admin backend in w3b>cms (aka w3blabor CMS) before 3.2.0 have unknown impact and remote attack vectors.	2009-02-17	10.0	CVE-2008-6158 CONFIRM
webbiscuits -- modules_controller	PHP remote file inclusion vulnerability in adminhead.php in WebBiscuits Modules Controller 1.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path[docroot] parameter.	2009-02-13	7.5	CVE-2008-6138 BID MILW0RM
wikkitikkitavi -- wikkitikkitavi	Unrestricted file upload vulnerability in upload.php in WikkiTikkiTavi 1.11 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in img/.	2009-02-16	7.5	CVE-2009-0602 XF BID MILW0RM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
2532gigs -- 2532gigs	2532designs 2532lGigs 1.2.2 and earlier allows remote attackers to trigger a backup and obtain sensitive information via a direct request to backup.php, which creates backup.sql under the web root with insufficient access control.	2009-02-19	4.0	CVE-2008-6199 XF MILW0RM
acid -- analysis_console_for_intrusion_databases base -- basic_analysis_and_security_engine	Multiple cross-site scripting (XSS) vulnerabilities in (1) acid_qry_main.php in Analysis Console for Intrusion Databases (ACID) 0.9.6b20 and (2) base_qry_main.php in Basic Analysis and Security Engine (BASE) 1.2, and unspecified other console scripts in these products, allow remote attackers to inject arbitrary web script or HTML via	2009-02-18	4.3	CVE-2005-4878 OSVDB DEBIAN SECUNIA CONFIRM

	the sig[1] parameter and possibly other parameters, a different vulnerability than CVE-2007-6156.			
apmuthu -- phpskelsite	Cross-site scripting (XSS) vulnerability in index.php in phpSkelSite 1.4 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2009-02-16	4.3	CVE-2009-0594 BID MILW0RM SECUNIA
avaya -- ip_soft_phone	Unspecified vulnerability in Avaya IP Softphone 6.0 SP4 and 6.01.85 allows remote attackers to cause a denial of service (crash) via a large amount of H.323 data.	2009-02-13	5.0	CVE-2008-6141 MISC BID CONFIRM SECUNIA
bookingcentre -- booking_system_for_hotels_group	Cross-site scripting (XSS) vulnerability in cadena_ofertas_ext.php in Venalsur Booking center Booking System for Hotels Group allows remote attackers to inject arbitrary web script or HTML via the OfertaID parameter.	2009-02-20	4.3	CVE-2008-6215 MILW0RM
brickhost -- phpscheduleit	Eval injection vulnerability in reserve.php in phpScheduleIt 1.2.10 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via the start_date parameter.	2009-02-13	6.8	CVE-2008-6132 XF BID MILW0RM SECUNIA
clip-share -- clipshare	Cross-site scripting (XSS) vulnerability in fullscreen.php in ClipShare Pro 4.0 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2009-02-19	4.3	CVE-2008-6173 BID SECUNIA MISC
d.j.bernstein -- djbdns	dnscache in Daniel J. Bernstein djbdns 1.05 does not prevent simultaneous identical outbound DNS queries, which makes it easier for remote attackers to spoof DNS responses, as demonstrated by a spoofed A record in the Additional section of a response to a Start of Authority (SOA) query.	2009-02-19	6.4	CVE-2008-4392 MISC

dminnich -- simple_php_news	Static code injection vulnerability in post.php in Simple PHP News 1.0 final allows remote attackers to inject arbitrary PHP code into news.txt via the post parameter, and then execute the code via a direct request to display.php. NOTE: some of these details are obtained from third party information.	2009-02-20	5.1	CVE-2009-0643 MILW0RM FRSIRT SECUNIA OSVDB
dreamcost -- hostadmin	Cross-site scripting (XSS) vulnerability in index.php in DreamCost HostAdmin 3.1.1 allows remote attackers to inject arbitrary web script or HTML via the page parameter.	2009-02-20	4.3	CVE-2008-6164 BID BUGTRAQ
drupal -- semantically_interconnected_online_communities	Semantically-Interconnected Online Communities (SIOC) 5.x before 5.x-1.2 and 6.x before 6.x-1.1, a module for Drupal, does not properly implement menu and database APIs, which allows remote attackers to obtain usernames and read hashed emails and comments via unspecified vectors.	2009-02-18	5.0	CVE-2008-6160 CONFIRM
drupal -- localization_client drupal -- localization_server	Cross-site request forgery (CSRF) vulnerability in the Localization client 5.x before 5.x-1.1 and 6.x before 6.x-1.6 and the Localization server 5.x before 5.x-1.0-alpha5 and 6.x before 6.x-alpha2, modules for Drupal, allows remote attackers to perform unauthorized actions as administrators via unspecified vectors related to the "local translation submission interface."	2009-02-19	6.8	CVE-2008-6169 CONFIRM
e107 -- e107	Cross-site scripting (XSS) vulnerability in submitnews.php in e107 CMS 0.7.11 allows remote attackers to inject arbitrary web script or HTML via the (1) author_name, (2)	2009-02-	4.3	CVE-2008-6208 XF

e107 -- e107	itemtitle, and (3) item parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	19	4.3	XF BID MISC
easy-script -- cspartner	SQL injection vulnerability in gestion.php in CSPartner 0.1, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the (1) pseudo and (2) passe parameters.	2009-02-18	6.8	CVE-2008-6165 MILW0RM SECUNIA
eeb-welt -- eebcms	Cross-site scripting (XSS) vulnerability in index.php in EEBCMS 0.95 allows remote attackers to inject arbitrary web script or HTML via the content parameter.	2009-02-19	4.3	CVE-2008-6190 XF BID MISC
extrakt -- extrakt_framework	Cross-site scripting (XSS) vulnerability in index.php in Extrakt Framework 0.7 allows remote attackers to inject arbitrary web script or HTML via the plugins[file][id] parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-20	4.3	CVE-2008-6217 XF MISC BID
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	6.2	CVE-2009-0360 FRSIRT
	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	2009-02		CVE-2009-

eyrie -- pam-krb5	users to overwrite and change the ownership of arbitrary files by setting the KRB5CCNAME environment variable, and then launching a setuid application that performs certain pam_setcred operations.	2009-02-13	4.6	0361 FRSIRT
falt4 -- falt4_extreme	Multiple cross-site request forgery (CSRF) vulnerabilities in the manage_users handler in admin/index.php in Falt4 CMS (aka Falt4 Extreme) RC4 allow remote attackers to change passwords as administrators via (1) edit and (2) edit_now actions.	2009-02-19	6.8	CVE-2009-0648 SECUNIA MISC
formfields -- adman	SQL injection vulnerability in editCampaign.php in AdMan 1.1.20070907 allows remote authenticated users to execute arbitrary SQL commands via the campaignId parameter.	2009-02-16	6.5	CVE-2008-6156 BID MILW0RM SECUNIA
hans_oesterholt -- cmme	Content Management Made Easy (CMME) 1.19 allows remote attackers to obtain system information via a direct request to info.php, which invokes the phpinfo function.	2009-02-18	5.0	CVE-2008-6159 XF BUGTRAQ MISC SECUNIA
ibm -- websphere_application_server	Unspecified vulnerability in the Performance Monitoring Infrastructure (PMI) feature in the Servlet Engine/Web Container component in IBM WebSphere Application Server (WAS) 6.1.x before 6.1.0.19, when a component statistic is enabled, allows attackers to cause a denial of service (daemon crash) via vectors related to "a gradual degradation in performance."	2009-02-17	5.0	CVE-2008-4285 CONFIRM AIXAPAR
	Directory traversal vulnerability in index.php in Jaws 0.8.8 allows remote authenticated users to read arbitrary files via a	2009-02		CVE-2009-

jaws -- jaws	.. (dot dot) in the (1) language, (2) Introduction_complete, and (3) use_log parameters, different vectors than CVE-2004-2445.	2009-02-18	6.5	0645 MISC
jetbox -- jetbox_cms	Cross-site scripting (XSS) vulnerability in admin/postlister/index.php in Jetbox CMS 2.1 allows remote attackers to inject arbitrary web script or HTML via the liste parameter.	2009-02-19	4.3	CVE-2008-6174 BID MISC
joomla -- rwcards	Directory traversal vulnerability in captcha/captcha_image.php in the RWCards (com_rwcards) 3.0.11 component for Joomla!, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the img parameter.	2009-02-19	6.8	CVE-2008-6172 BID MILW0RM SECUNIA
k2sxs -- silvershield	SilverSHielD 1.0.2.34 allows remote attackers to cause a denial of service (application crash) via a crafted argument to the opendir SFTP command.	2009-02-19	5.0	CVE-2008-6175 BID MILW0RM SECUNIA
kwsphp -- kwsphp	Directory traversal vulnerability in help.php in the eskuel module in KwsPHP 1.3.456, as available before 20080416, allows remote attackers to execute arbitrary commands via the action parameter. NOTE: some of these details are obtained from third party information.	2009-02-19	6.8	CVE-2008-6201 FRSIRT SECUNIA MILW0RM CONFIRM
linux -- kernel	Stack consumption vulnerability in the do_page_fault function in arch/x86/mm/fault.c in the Linux kernel before 2.6.28.5 allows local users to cause a denial of service (memory corruption) or possibly gain privileges via unspecified vectors that trigger page faults on a	2009-02-17	4.9	CVE-2009-0605 BID

	machine that has a registered Kprobes probe.			
mcgallerypro -- mcgallery	Multiple cross-site scripting (XSS) vulnerabilities in PhpForums.net mcGallery 1.1 allow remote attackers to inject arbitrary web script or HTML via the lang parameter to (1) admin.php, (2) index.php, (3) sess.php, (4) stats.php, (5) detail.php, (6) resize.php, and (7) show.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	4.3	CVE-2008-6211 XF BID MISC MISC
microsoft -- windows_live_messenger	msnmsgr.exe in Windows Live Messenger (WLM) 2009 build 14.0.8064.206, and other 14.0.8064.x builds, allows remote attackers to cause a denial of service (application crash) via a modified header in a packet, as possibly demonstrated by a UTF-8.0 value of the charset field in the Content-Type header line.	2009-02-19	5.0	CVE-2009-0647 BID BUGTRAQ
miniportail -- miniportail	Cross-site scripting (XSS) vulnerability in search.php in miniPortail 2.2 and earlier allows remote attackers to inject arbitrary web script or HTML via an unspecified argument, probably the search string.	2009-02-19	4.3	CVE-2008-6168 BID MILW0RM
mozilo -- mozilowiki	Directory traversal vulnerability in print.php in moziloWiki 1.0.1 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the page parameter.	2009-02-13	4.3	CVE-2008-6129 CONFIRM
myblog -- myblog	Sam Crew MyBlog stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.	2009-02-19	5.0	CVE-2008-6193 MILW0RM
	Directory traversal vulnerability in send.php in			

ninjadesigns -- mailist	Ninja Designs Mailist 3.0, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the load parameter. NOTE: some of these details are obtained from third party information.	2009-02-13	5.1	CVE-2009-0570 BID MILW0RM SECUNIA
ninjadesigns -- mailist	admin.php in Ninja Designs Mailist 3.0 stores backup copies of maillist.php under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to the backup directory.	2009-02-13	5.0	CVE-2009-0571 MILW0RM SECUNIA
noticeware -- noticeware_email_server_ng	NoticeWare Email Server NG 5.1.2.2 allows remote attackers to cause a denial of service (crash) via multiple POP3 requests with a long PASS command.	2009-02-19	5.0	CVE-2008-6185 XF BID MILW0RM FRSIRT SECUNIA
novell -- open_enterprise_server	Multiple cross-site scripting (XSS) vulnerabilities in qfsearch/AdminServlet in QuickFinder Server in Novell Open Enterprise Server 1.x allow remote attackers to inject arbitrary web script or HTML via (1) the siteloc parameter in a displayaddsite action, the site parameter in a (2) generalproperties or (3) clusterserviceproperties action, (4) the adminurl parameter in a global action, or (5) the print-list parameter.	2009-02-17	4.3	CVE-2009-0611 XF SECTRACK BID FRSIRT SECUNIA MISC OSVDB
php-stats -- php-stats	Cross-site scripting (XSS) vulnerability in admin.php in Php-Stats 0.1.9.1 allows remote attackers to inject arbitrary web script or HTML via the (1) sel_mese and (2) sel_anno parameters in a systems	2009-02-19	4.3	CVE-2008-6212 XF MISC

	action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.			BID MISC
phpskelsite -- phpskelsite	PHP remote file inclusion vulnerability in skysilver/login.tpl.php in phpSkelSite 1.4, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary PHP code via a URL in the theme parameter.	2009-02-16	5.1	CVE-2009-0595 BID MILW0RM SECUNIA
phpskelsite -- phpskelsite	Directory traversal vulnerability in skysilver/login.tpl.php in phpSkelSite 1.4, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the TplSuffix parameter.	2009-02-16	6.8	CVE-2009-0596 BID MILW0RM SECUNIA
plxwebdev -- plx_auto_reminder	SQL injection vulnerability in members.php in plx Auto Reminder 3.7 allows remote authenticated users to execute arbitrary SQL commands via the id parameter in a newar action.	2009-02-16	6.5	CVE-2009-0593 BID MILW0RM SECUNIA
publicwarehouse -- lightblog	Multiple directory traversal vulnerabilities in LightBlog 9.8, when magic_quotes_gpc is disabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) username parameter to view_member.php, (2) username_post parameter to login.php, and the (3) Lightblog_username cookie parameter to check_user.php.	2009-02-19	6.8	CVE-2008-6177 BID MILW0RM SECUNIA
	ext/openssl/ossl_ocsp.c in Ruby 1.8 and 1.9 does not properly check the return value from the OCSP_basic_verify	2009-02		CVE-2009-0642 XF

ruby-lang -- ruby	function, which might allow remote attackers to successfully present an invalid X.509 certificate, possibly involving a revoked certificate.	2009-02-20	6.8	XF BID CONFIRM MISC
sepcity -- classified_ads	SepCity Classified Ads stores the admin password in cleartext in data/classifieds.mdb, which allows context-dependent attackers to obtain sensitive information.	2009-02-17	5.0	CVE-2008-6157 MILW0RM
sourceforge -- wow_raid_manager	Cross-site scripting (XSS) vulnerability in WOW Raid Manager (WRM) before 3.5.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-02-18	4.3	CVE-2008-6161 CONFIRM CONFIRM
sun -- java_system_portal_server	Multiple cross-site scripting (XSS) vulnerabilities in unspecified Portlets in Sun Java System Portal Server 7.0 and 7.1 allow remote attackers to inject arbitrary web script or HTML via unknown vectors.	2009-02-19	4.3	CVE-2008-6192 BID SUNALERT
swannsecurity -- dvr4-securanet	The HTTP interface in Swann DVR4-SecuraNet has a certain default administrative username and password, which makes it easier for remote attackers to obtain privileged access.	2009-02-18	5.0	CVE-2009-0644 BUGTRAQ MISC
swannsecurity -- dvr4-securanet	Directory traversal vulnerability in the administrative web server in Swann DVR4-SecuraNet allows remote attackers to read arbitrary files via a .. (dot dot) in the URI, as demonstrated by reading the vy_netman.cfg file that contains passwords.	2009-02-20	5.0	CVE-2009-0640 BID BUGTRAQ SECUNIA MISC OSVDB
trend_micro -- interscan_web_security_suite	Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 3.x and InterScan Web Security Suite (IWSS) 3.x, when basic authorization is enabled on the standalone	2009-02		CVE-2009-0612 XF

trend_micro -- interscan_web_security_virtual_appliance	proxy, forwards the Proxy-Authorization header from Windows Media Player, which allows remote web servers to obtain credentials by offering a media stream and then capturing this header.	2009-02-17	4.3	SECTRACK BID BUGTRAQ SECUNIA
trend_micro -- interscan_web_security_suite	Trend Micro InterScan Web Security Suite (IWSS) 3.1 before build 1237 allows remote authenticated Auditor and Report Only users to bypass intended permission settings, and modify the system configuration, via requests to unspecified JSP pages.	2009-02-17	6.0	CVE-2009-0613 FRSIRT
w3b_cms -- aka_w3blabor_cms	SQL injection vulnerability in admin/index.php in w3b>cms (aka w3blabor CMS) before 3.4.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the benutzername parameter (aka Username field) in a login action.	2009-02-16	6.8	CVE-2009-0597 BID
wiki -- swiki	Multiple cross-site scripting (XSS) vulnerabilities in Swiki 1.5 allow remote attackers to inject arbitrary web script or HTML via (1) the query string and (2) a new wiki entry.	2009-02-19	4.3	CVE-2008-6200 BID BUGTRAQ
wireshark -- wireshark	Buffer overflow in wiretap/netscreen.c in Wireshark 0.99.7 through 1.0.5 allows user-assisted remote attackers to cause a denial of service (application crash) via a malformed NetScreen snoop file.	2009-02-16	5.0	CVE-2009-0599 BID FRSIRT
wireshark -- wireshark	Wireshark 0.99.6 through 1.0.5 allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted Tektronix K12 text capture file, as demonstrated by a file with exactly one frame.	2009-02-16	4.3	CVE-2009-0600 FRSIRT

xaaaaav38 -- urlstreet	Cross-site scripting (XSS) vulnerability in seeurl.php in Xavier Flahaut URLStreet 1.0 allows remote attackers to inject arbitrary web script or HTML via the (1) language, (2) order, and (3) filter parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-19	4.3	CVE-2008-6205 XF BID MISC

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
drupal -- link_module	Cross-site scripting (XSS) vulnerability in index.php in the Link module 5.x-2.5 for Drupal 5.10 allows remote authenticated users, with "administer content types" privileges, to inject arbitrary web script or HTML via the description parameter (aka the Help field). NOTE: some of these details are obtained from third party information.	2009-02-16	3.5	CVE-2009-0603 XF BID SECUNIA OSVDB FULLDISC
drupal -- drupal	Cross-site scripting (XSS) vulnerability in Drupal 5.x before 5.12 and 6.x before 6.6, allows remote authenticated users with create book content or edit node book hierarchy permissions to inject arbitrary web script or HTML via the book page title.	2009-02-19	3.5	CVE-2008-6170 CONFIRM
ibm -- websphere_message_broker	IBM WebSphere Message Broker 6.1.x before 6.1.0.2 writes a database connection password to the Event Log and System Log during exception handling for a JDBC error, which allows local users to obtain sensitive information by reading these logs.	2009-02-13	2.1	CVE-2009-0503 CONFIRM
ibm -- websphere_application_server	WSPolicy in the Web Services component in IBM WebSphere Application Server (WAS) 7.0.x before 7.0.0.1 does not properly recognize the IDAssertion.isUsed binding property, which allows local users to discover a password by reading a SOAP message.	2009-02-17	2.1	CVE-2009-0504 CONFIRM
intrinsic -- swimage_encore	Conductor.exe in Intrinsic Swimage Encore before 5.0.1.21 contains a hardcoded password, which might allow local users to decrypt certain .bin files. NOTE: it is not clear whether this issue crosses privilege boundaries.	2009-02-19	2.1	CVE-2008-6191 CERT-VN BID
	Multiple cross-site scripting (XSS) vulnerabilities in Samizdat before 0.6.2	2009-02		CVE-2009-0359

nongnu -- samizdat	allow remote authenticated users to inject arbitrary web script or HTML via the (1) message title or (2) user full name.	2009-02-17	3.5	0339 BID CONFIRM
wireshark -- wireshark	Format string vulnerability in Wireshark 0.99.8 through 1.0.5 on non-Windows platforms allows local users to cause a denial of service (application crash) via format string specifiers in the HOME environment variable.	2009-02-16	2.1	CVE-2009-0601 BID FRSIRT

Back to top