

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	Discovered Published	CVSS Score	Source & Patch Info
Adobe -- Acrobat 3D Adobe -- Acrobat Reader	Unspecified vulnerability in Adobe Reader and Acrobat 7.0.9 and earlier, and 8.0 through 8.1.2, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors, related to an "input validation issue in a JavaScript method."	unknown 2008-06-25	10.0	CVE-2008-2641 OTHER-REF
AJ Square -- aj_auction	SQL injection vulnerability in category.php in AJSquare AJ Auction Pro web 2.0 allows remote attackers to execute arbitrary SQL commands via the cate_id parameter.	unknown 2008-06-25	7.5	CVE-2008-2860 MILWORM BID
ajhyip -- aj_square_aj-hyip	SQL injection vulnerability in news.php in AJ Square aj-hyip (aka AJ HYIP Acme) allows remote attackers to execute arbitrary SQL commands via the id parameter, a different vector than CVE-2008-2532.	unknown 2008-06-27	7.5	CVE-2008-2893 MILWORM BID
aprox -- aproxengine	Directory traversal vulnerability in index.php in AproxEngine 5.1.0.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.	unknown 2008-06-27	7.5	CVE-2008-2895 MILWORM BID
Aspindir -- shibby_shop	SQL injection vulnerability in default.asp in sHibby sHop 2.2 and earlier allows remote attackers to execute arbitrary SQL commands via the sayfa parameter.	unknown 2008-06-26	7.5	CVE-2008-2872 MILWORM BID XF
Aspindir -- shibby_shop	upgrade.asp in sHibby sHop 2.2 and earlier does not require administrative authentication, which allows remote attackers to update a file or have unspecified other impact via a direct request.	unknown 2008-06-26	7.5	CVE-2008-2882 MILWORM XF
boatscripts -- boatscripts_classifieds	SQL injection vulnerability in index.php in BoatScripts Classifieds allows remote attackers to execute arbitrary SQL commands via the type parameter.	unknown 2008-06-25	7.5	CVE-2008-2846 MILWORM BID XF
carscripts -- carscripts_classifieds	SQL injection vulnerability in index.php in Carscripts Classifieds allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-06-25	7.5	CVE-2008-2844 MILWORM BID XF
Caupo.net -- caupoShop_classic	SQL injection vulnerability in csc_article_details.php in Caupo.net CaupoShop Classic 1.3 allows remote attackers to execute arbitrary SQL commands via the saArticle[ID] parameter.	unknown 2008-06-25	7.5	CVE-2008-2866 MILWORM BID XF

Cisco -- Unified Communications Manager Cisco -- Unified CallManager	The Computer Telephony Integration (CTI) Manager service in Cisco Unified Communications Manager (CUCM) 5.x before 5.1(3c) and 6.x before 6.1(2) allows remote attackers to cause a denial of service (TSP crash) via malformed network traffic to TCP port 2748.	unknown 2008-06-26	7.8	CVE-2008-2061
cms.brdconcept -- cms-brd	SQL injection vulnerability in index.php in CMS-BRD allows remote attackers to execute arbitrary SQL commands via the menuclick parameter.	unknown 2008-06-24	7.5	CVE-2008-2837 MILWORM BID XF
doitlive -- cms	Multiple SQL injection vulnerabilities in doITLive CMS 2.50 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) ID parameter in an USUB action to default.asp and the (2) Licence[SpecialLicenseNumber] (aka LicenceId) cookie to edit/default.asp.	unknown 2008-06-25	7.5	CVE-2008-2843 MILWORM OTHER-REF BID XF XF
Drupal -- trailscout_module	SQL injection vulnerability in the TrailScout module 5.x before 5.x-1.4 for Drupal allows remote attackers to execute arbitrary SQL commands via unspecified cookies, related to improper use of the Drupal database API.	unknown 2008-06-25	7.5	CVE-2008-2850 BID XF
DUware -- DUcalendar	SQL injection vulnerability in detail.asp in DUware DUcalendar 1.0 and possibly earlier allows remote attackers to execute arbitrary SQL commands via the iEve parameter.	unknown 2008-06-26	7.5	CVE-2008-2868 MILWORM BID
e-topbiz -- viral_dx_1	SQL injection vulnerability in adclick.php in E-topbiz Viral DX 1 2.07 allows remote attackers to execute arbitrary SQL commands via the bannerid parameter.	unknown 2008-06-26	7.5	CVE-2008-2867 MILWORM BID
e-topbiz -- link_ads_1	SQL injection vulnerability in out.php in E-topbiz Link ADS 1 allows remote attackers to execute arbitrary SQL commands via the linkid parameter.	unknown 2008-06-26	7.5	CVE-2008-2869 MILWORM BID
easy_webstore -- easy_webstore	SQL injection vulnerability in index.php in Easy Webstore 1.2 allows remote attackers to execute arbitrary SQL commands via the cat_path parameter.	unknown 2008-06-25	7.5	CVE-2008-2853 MILWORM BID
elinestudio -- site_composer	Multiple SQL injection vulnerabilities in eLineStudio Site Composer (ESC) 2.6 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to ansFAQ.asp and the (2) template_id parameter to preview.asp.	unknown 2008-06-25	7.5	CVE-2008-2862 BUGTRAQ MILWORM OTHER-REF BID XF
elinestudio -- site_composer	Multiple absolute path traversal vulnerabilities in eLineStudio Site Composer (ESC) 2.6 allow remote attackers to create or delete arbitrary directories via a full pathname in the inpCurrFolder parameter to (1) folderdel_.asp or (2) foldernew.asp in cms/assetmanager/.	unknown 2008-06-25	7.5	CVE-2008-2863 BUGTRAQ MILWORM OTHER-REF BID XF
eMuSOFT -- emuCMS	SQL injection vulnerability in index.php in eMuSOFT emuCMS 0.3 allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a category action.	unknown 2008-06-27	7.5	CVE-2008-2891 MILWORM BID
feellove -- exp_shop_component	SQL injection vulnerability in the EXP Shop (com_expshop) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter in a show_payment action to index.php.	unknown 2008-06-27	7.5	CVE-2008-2892 MILWORM BID
fullrevolution -- aspwebcalendar2008	Unrestricted file upload vulnerability in calendar_admin.asp in Full Revolution aspWebCalendar 2008 allows remote attackers to upload and execute arbitrary code via the FILE1 parameter in an uploadfileprocess action, probably followed by a direct request to the file in calendar/eventimages/.	unknown 2008-06-24	10.0	CVE-2008-2832 OTHER-REF BID XF
getfireant -- fireant	Directory traversal vulnerability in index.php in FireAnt 1.3 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.	unknown 2008-06-27	7.5	CVE-2008-2896 MILWORM BID XF

IBM -- afp_viewer_plug-in	Heap-based buffer overflow in the IBM AFP Viewer Plug-in 2.0.7.1 and 3.2.1.1 allows remote attackers to execute arbitrary code via a long SRC property value. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-26	9.3	CVE-2008-2880
j00lean-cms -- j00lean-cms	Unspecified vulnerability in includes/classes/page.php in j00lean-CMS 1.03 has unknown impact and attack vectors.	unknown 2008-06-27	10.0	CVE-2008-2899
Jamroom -- Jamroom	PHP remote file inclusion vulnerability in include/plugins/jrBrowser/payment.php in Jamroom 3.3.0 through 3.3.5 allows remote attackers to execute arbitrary PHP code via a URL in the jamroom[jm_dir] parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-06-26	7.5	CVE-2008-2883 MILWORM OTHER-REF OTHER-REF
Jamroom -- Jamroom	PHP remote file inclusion vulnerability in include/plugins/jrBrowser/purchase.php in Jamroom 3.3.0 through 3.3.5, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the jamroom[jm_dir] parameter.	unknown 2008-06-27	9.3	CVE-2008-2886 MILWORM OTHER-REF BID
k5n -- WebCalendar	PHP remote file inclusion vulnerability in send_reminders.php in WebCalendar 1.0.4 allows remote attackers to execute arbitrary PHP code via a URL in the includedir parameter and a 0 value for the noSet parameter, a different vector than CVE-2007-1483.	unknown 2008-06-24	7.5	CVE-2008-2836 MILWORM MLIST BID XF
Kalptaru Infotech -- php_site_lock	SQL injection vulnerability in index.php in Kalptaru Infotech PHP Site Lock 2.0 allows remote attackers to execute arbitrary SQL commands via the articleid parameter in a show_article action.	unknown 2008-06-25	7.5	CVE-2008-2865 MILWORM BID
migcms -- migcms	Multiple PHP remote file inclusion vulnerabilities in MiGCMS 2.0.5, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[application][app_root] parameter to (1) collection.class.php and (2) content_image.class.php in lib/obj/.	unknown 2008-06-27	9.3	CVE-2008-2888 MILWORM BID
munky -- munky	Directory traversal vulnerability in index.php in mUnky 0.0.1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the zone parameter.	unknown 2008-06-26	7.5	CVE-2008-2876 MILWORM
mybizz-classifieds -- mybizz-classifieds	SQL injection vulnerability in index.php in MyBizz-Classifieds allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-06-25	7.5	CVE-2008-2845 MILWORM BID
odars -- odars	PHP remote file inclusion vulnerability in src/browser/resource/categories/resource_categories_view.php in Open Digital Assets Repository System (ODARS) 1.0.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the CLASSES_ROOT parameter.	unknown 2008-06-27	9.3	CVE-2008-2885 MILWORM
offl -- online_fantasy_football_league	Multiple SQL injection vulnerabilities in Online Fantasy Football League (OFFL) 0.2.6 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) fflteam_id parameter to teams.php, the (2) league_id parameter to leagues.php, and the (3) player_id parameter to players.php.	unknown 2008-06-27	7.5	CVE-2008-2890 MILWORM BID
offsystem -- offsystem	Multiple buffer overflows in OFF System before 0.19.14 allow remote attackers to have an unknown impact via unspecified vectors related to "parsing of http headers."	unknown 2008-06-25	10.0	CVE-2008-2851 OTHER-REF XF
orlando_cms -- orlando_cms	Multiple PHP remote file inclusion vulnerabilities in Orlando CMS 0.6 allow remote attackers to execute arbitrary PHP code via a URL in the GLOBALS[preloc] parameter to (1) modules/core/logger/init.php and (2) AJAX/newscat.php.	unknown 2008-06-25	7.5	CVE-2008-2854 MILWORM BID XF

ownrs -- ownrs	SQL injection vulnerability in clanek.php in OwnRS Beta 3 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-25	7.5	CVE-2008-2856 MILWORM BID XF
pagesperso-orange -- gfl_sdk pagesperso-orange -- xnview pagesperso-orange -- nconvert	Stack-based buffer overflow in NConvert 4.92, GFL SDK 2.82, and XnView 1.93.6 on Windows and 1.70 on Linux and FreeBSD allows user-assisted remote attackers to execute arbitrary code via a crafted format keyword in a Sun TAAC file.	unknown 2008-06-24	9.3	CVE-2008-2427 BUGTRAQ BID SECTRACK
pagesquid -- pagesquid_cms	SQL injection vulnerability in index.php in PageSquid CMS 0.3 Beta allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2008-06-27	7.5	CVE-2008-2897 MILWORM BID
PHPauction -- PHPauction	SQL injection vulnerability in item.php in PHPAuction 3.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-27	7.5	CVE-2008-2900 MILWORM BID
rss_aggregator -- rss_aggregator	PHP remote file inclusion vulnerability in display.php in RSS-aggregator allows remote attackers to execute arbitrary PHP code via a URL in the path parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-06-27	9.3	CVE-2008-2884 MILWORM
ruby-lang -- Ruby	Multiple integer overflows in the rb_str_buf_append function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, 1.8.7 before 1.8.7-p22, and 1.9.0 before 1.9.0-2 allow context-dependent attackers to execute arbitrary code or cause a denial of service via unknown vectors that trigger memory corruption, a different issue than CVE-2008-2663, CVE-2008-2664, and CVE-2008-2725. NOTE: as of 20080624, there has been inconsistent usage of multiple CVE identifiers related to Ruby. This CVE description should be regarded as authoritative, although it is likely to change.	unknown 2008-06-24	10.0	CVE-2008-2662 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF
ruby-lang -- Ruby	Multiple integer overflows in the rb_ary_store function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, and 1.8.7 before 1.8.7-p22 allow context-dependent attackers to execute arbitrary code or cause a denial of service via unknown vectors, a different issue than CVE-2008-2662, CVE-2008-2664, and CVE-2008-2725. NOTE: as of 20080624, there has been inconsistent usage of multiple CVE identifiers related to Ruby. The CVE description should be regarded as authoritative, although it is likely to change.	unknown 2008-06-24	10.0	CVE-2008-2663 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF
ruby-lang -- Ruby	The rb_str_format function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, 1.8.7 before 1.8.7-p22, and 1.9.0 before 1.9.0-2 allows context-dependent attackers to trigger memory corruption via unspecified vectors related to alloca, a different issue than CVE-2008-2662, CVE-2008-2663, and CVE-2008-2725. NOTE: as of 20080624, there has been inconsistent usage of multiple CVE identifiers related to Ruby. The CVE description should be regarded as authoritative, although it is likely to change.	unknown 2008-06-24	7.8	CVE-2008-2664 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF
ruby-lang -- Ruby	Integer overflow in the rb_ary_splice function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, and 1.8.7 before 1.8.7-p22 allows context-dependent attackers to trigger memory corruption via unspecified vectors, aka the "REALLOC_N" variant, a different issue than CVE-2008-2662, CVE-2008-2663, and CVE-2008-2664. NOTE: as of 20080624, there has been inconsistent usage of multiple CVE identifiers related to Ruby. The CVE description should be regarded as authoritative, although it is likely to change.	unknown 2008-06-24	7.8	CVE-2008-2725 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF

ruby-lang -- Ruby	Integer overflow in the rb_ary_splice function in Ruby 1.8.4 and earlier, 1.8.5 before 1.8.5-p231, 1.8.6 before 1.8.6-p230, 1.8.7 before 1.8.7-p22, and 1.9.0 before 1.9.0-2 allows context-dependent attackers to trigger memory corruption, aka the "beg + rlen" issue. NOTE: as of 20080624, there has been inconsistent usage of multiple CVE identifiers related to Ruby. The CVE description should be regarded as authoritative, although it is likely to change.	unknown 2008-06-24	7.8	CVE-2008-2726 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF
sharecms -- sharecms	Multiple SQL injection vulnerabilities in ShareCMS 0.1 Beta allow remote attackers to execute arbitrary SQL commands via the (1) eventID parameter to event_info.php and the (2) userID parameter to list_user.php.	unknown 2008-06-26	7.5	CVE-2008-2870 MILWORM BID XF
sidb -- scientific_image_database	SQL injection vulnerability in projects.php in Scientific Image DataBase 0.41 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-24	7.5	CVE-2008-2834 MILWORM BID XF
softbizscripts -- softbiz_jokes_and_funny_pics_script	SQL injection vulnerability in index.php in Softbiz Jokes & Funny Pics Script allows remote attackers to execute arbitrary SQL commands via the sbjoke_id parameter, a different vector than CVE-2008-1050.	unknown 2008-06-26	7.5	CVE-2008-2874 MILWORM
softdivision -- maxtrade_aoi	SQL injection vulnerability in the Trade module in Maxtrade AIO 1.3.23 allows remote attackers to execute arbitrary SQL commands via the categori parameter in a pocategorisell action to modules.php.	unknown 2008-06-25	7.5	CVE-2008-2847 MILWORM BID
webdevindo-cms -- webdevindo-cms	SQL injection vulnerability in index.php in Webdevindo-CMS 1.0.0 allows remote attackers to execute arbitrary SQL commands via the hal parameter.	unknown 2008-06-26	7.5	CVE-2008-2875 MILWORM
worldlevel -- le.cms	admin/upload.php in le.cms 1.4 and earlier allows remote attackers to bypass administrative authentication, and upload and execute arbitrary files in images/, via a nonzero value for the submit0 parameter in conjunction with filenames in the filename and upload parameters.	unknown 2008-06-24	10.0	CVE-2008-2833 MILWORM BID BID

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
acebit -- wise_ftp	Directory traversal vulnerability in the FTP client in AceBIT WISE-FTP 4.1.0 and 5.5.8 allows remote FTP servers to create or overwrite arbitrary files via a ..\ (dot dot backslash) in a response to a LIST command, a related issue to CVE-2002-1345.	unknown 2008-06-27	6.8	CVE-2008-2889 OTHER-REF BID
AltraSoft -- AskMe Pro	AltraSoft AskMe Pro 2.1 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.	unknown 2008-06-25	5.0	CVE-2008-2857 MILWORM
Aspindir -- shibby_shop	sHibby sHop 2.2 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request to Db/urun.mdb.	unknown 2008-06-26	5.0	CVE-2008-2873 MILWORM XF
benjacms -- benja_cms	Benja CMS 0.1 does not require authentication for access to admin/, which allows remote attackers to add or delete a menu.	unknown 2008-06-26	5.0	CVE-2008-2879 BUGTRAQ BID
chaozzatwork -- fubarforum	Directory traversal vulnerability in index.php in chaozz@work FubarForum 1.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.	unknown 2008-06-27	5.0	CVE-2008-2887 MILWORM BID XF

Cisco -- Unified Communications Manager Cisco -- Unified CallManager	The Real-Time Information Server (RIS) Data Collector service in Cisco Unified Communications Manager (CUCM) before 4.2(3)SR4, and 4.3 before 4.3(2)SR1, allows remote attackers to bypass authentication, and obtain cluster configuration information and statistics, via a direct TCP connection to the service port, aka Bug ID CSCsq35151.	unknown 2008-06-26	5.0	CVE-2008-2062
Cisco -- Unified Communications Manager Cisco -- Unified CallManager	The Real-Time Information Server (RIS) Data Collector service in Cisco Unified Communications Manager (CUCM) 5.x before 5.1(3) and 6.x before 6.1(1) allows remote attackers to bypass authentication, and obtain cluster configuration information and statistics, via a direct TCP connection to the service port, aka Bug ID CSCsj90843.	unknown 2008-06-26	5.0	CVE-2008-2730
cmsworks -- cmsworks	PHP remote file inclusion vulnerability in admin/include/lib.module.php in cmsWorks 2.2 RC4, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mod_root parameter.	unknown 2008-06-26	6.8	CVE-2008-2877 MILWORM BID XF
doitlive -- cms	Cross-site scripting (XSS) vulnerability in edit/showmedia.asp in doITLive CMS 2.50 and earlier allows remote attackers to inject arbitrary web script or HTML via the FILE parameter.	unknown 2008-06-25	4.3	CVE-2008-2842 MILWORM OTHER-REF BID XF
elinestudio -- site_composer	Multiple cross-site scripting (XSS) vulnerabilities in eLineStyle Studio Site Composer (ESC) 2.6 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) topic and (2) button parameters to ansFAQ.asp and the (3) id and (4) txtEmail parameters to login.asp.	unknown 2008-06-25	4.3	CVE-2008-2861 BUGTRAQ MILWORM BID XF
elinestudio -- site_composer	eLineStyle Studio Site Composer (ESC) 2.6 and earlier allows remote attackers to obtain sensitive information via a direct request to (1) trigger.asp or (2) common2.asp in cms/include/, which reveals the database path.	unknown 2008-06-25	5.0	CVE-2008-2864 BUGTRAQ MILWORM OTHER-REF XF
exerocms -- exero_cms	Multiple directory traversal vulnerabilities in Exero CMS 1.0.0 and 1.0.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the theme parameter to (1) custompage.php, (2) errors/404.php, (3) members/memberslist.php, (4) members/profile.php, (5) news/fullview.php, (6) news/index.php, (7) nopermision.php, (8) usercp/avatar.php, or (9) usercp/editpassword.php in themes/Default/. NOTE: some of these details are obtained from third party information.	unknown 2008-06-24	6.8	CVE-2008-2840 OTHER-REF
hedgehog-cms -- hedgehog-cms	Directory traversal vulnerability in includes/header.php in Hedgehog-CMS 1.21 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the c_temp_path parameter. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2.sftp URL.	unknown 2008-06-27	6.8	CVE-2008-2898 MILWORM
igsuite -- igsuite	SQL injection vulnerability in cgi-bin/igsuite in IGSuite 3.2.4 allows remote attackers to execute arbitrary SQL commands via the formid parameter.	unknown 2008-06-24	6.8	CVE-2008-2835 MILWORM BID XF
Microsoft -- ie XChat -- XChat	Argument injection vulnerability in XChat 2.8.7b and earlier on Windows, when Internet Explorer is used, allows remote attackers to execute arbitrary commands via the --command parameter in an ircs:// URI.	unknown 2008-06-24	6.8	CVE-2008-2841 MILWORM OTHER-REF
Mindtouch -- DekiWiki	Cross-site scripting (XSS) vulnerability in the search functionality in MindTouch DekiWiki before 8.05.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-25	4.3	CVE-2008-2848 OTHER-REF XF

Nathan Neulinger -- CGIWrap	Cross-site scripting (XSS) vulnerability in CGIWrap before 4.1, when an Internet Explorer based browser is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to failure to set the charset in error messages.	unknown 2008-06-25	4.3	CVE-2008-2852 OTHER-REF BID XF
NCH Software -- nch_software_classic_ftp	Directory traversal vulnerability in the FTP client in NCH Software Classic FTP 1.02 for Windows allows remote FTP servers to create or overwrite arbitrary files via a .. (dot dot) in a response to a LIST command, a related issue to CVE-2002-1345.	unknown 2008-06-27	6.8	CVE-2008-2894 OTHER-REF BID XF
NetWin -- SurgeMail	Unspecified vulnerability in the IMAP service in NetWin SurgeMail before 3.9g2 allows remote attackers to cause a denial of service (daemon crash) via unknown vectors related to an "imap command."	unknown 2008-06-25	5.0	CVE-2008-2859 OTHER-REF BID XF
ownrs -- ownrs	Cross-site scripting (XSS) vulnerability in clanek.php in OwnRS Beta 3 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	unknown 2008-06-25	4.3	CVE-2008-2855 MILWORM BID XF
PEGames -- PEGames	Multiple cross-site scripting (XSS) vulnerabilities in template2.php in PEGames allow remote attackers to inject arbitrary web script or HTML via the (1) sitetitle, (2) sitenav, (3) sitemain, and (4) sitealt parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-26	4.3	CVE-2008-2871 BID XF
redhat -- enterprise_linux redhat -- desktop_workstation redhat -- desktop	Untrusted search path vulnerability in a certain Red Hat build script for Standards Based Linux Instrumentation for Manageability (sblim) libraries before 1-13a.el4_6.1 in Red Hat Enterprise Linux (RHEL) 4, and before 1-31.el5_2.1 in RHEL 5, allows local users to gain privileges via a malicious library in a certain subdirectory of /var/tmp, related to an incorrect RPATH setting, as demonstrated by a malicious libc.so library for tog-pegasus.	unknown 2008-06-25	4.6	CVE-2008-1951 OTHER-REF REDHAT
relative_real_estate_systems -- relative_real_estate_systems	Relative Real Estate Systems 3.0 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information.	unknown 2008-06-26	5.0	CVE-2008-2881 MILWORM OTHER-REF
traindepot -- traindepot	Directory traversal vulnerability in index.php in Traindepot 0.1 allows remote attackers to read arbitrary files via a .. (dot dot) in the module parameter.	unknown 2008-06-24	5.0	CVE-2008-2838 MILWORM BID XF
traindepot -- traindepot	Cross-site scripting (XSS) vulnerability in the search module in Traindepot 0.1 allows remote attackers to inject arbitrary web script or HTML via the query parameter to index.php.	unknown 2008-06-24	4.3	CVE-2008-2839 MILWORM BID XF
webchamado -- webchamado	SQL injection vulnerability in index.php in WebChamado 1.1 allows remote attackers to execute arbitrary SQL commands via the eml parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-25	6.8	CVE-2008-2858
yektaweb -- academic_web_tools	Open redirect vulnerability in rss_getfile.php in Academic Web Tools (AWT YEKTA) 1.4.3.1, and 1.4.2.8 and earlier, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the file parameter.	unknown 2008-06-26	6.4	CVE-2008-2878 BUGTRAQ OTHER-REF BID XF

[Back to top](#)

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
---------------------------	-------------	----------------------	------------	---------------------

Drupal -- trailscout_module	Cross-site scripting (XSS) vulnerability in the TrailScout module 5.x before 5.x-1.4 for Drupal allows remote authenticated users, with create post permissions, to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-25	3.5	CVE-2008-2849 OTHER-REF BID XF
-----------------------------	--	-----------------------	---------------------	---

[Back to top](#)