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**
phpbb -- Tag Board	SQL injection vulnerability in tag_board.php in the Tag Board module 4.0 and earlier for phpBB allows remote attackers to execute arbitrary SQL commands via the id parameter in a delete action.	2009-02-27	7.5	CVE-2008-6314 XF BID MILW0RM SECUNIA OSVDB
1scripts -- z1exchange	SQL injection vulnerability in edit.php in Z1Exchange 1.0 allows remote attackers to execute arbitrary SQL commands via the site parameter.	2009-02-25	7.5	CVE-2008-6284 XF BID MILW0RM
accscripts -- acc_php_email	Acc PHP eMail 1.1 allows remote attackers to bypass authentication and gain administrative access by setting the NEWSLETTERLOGIN cookie to "admin".	2009-02-26	7.5	CVE-2008-6291 XF BID MILW0RM SECUNIA
accscripts -- acc_autos	Acc Autos 4.0 allows remote attackers to bypass authentication and gain administrative access by setting the (1) username_cookie to "admin," (2) right_cookie to "1," and (3) id_cookie to "1."	2009-02-26	7.5	CVE-2008-6292 XF BID MILW0RM SECUNIA
	admin/Index.php in Acc			CVE-2008

accscripts -- acc_real_estate	Real Estate 4.0 allows remote attackers to bypass authentication and gain administrative access by setting the username_cookie to "admin."	2009-02-26	7.5	CVE-2008-6293 XF BID MILW0RM SECUNIA
accscripts -- acc_statistics	admin/Index.php in Acc Statistics 1.1 allows remote attackers to bypass authentication and gain administrative access by setting the username_cookie cookie to "admin."	2009-02-26	7.5	CVE-2008-6294 BID MILW0RM SECUNIA
activewebsoftwares -- active_newsletter	Multiple SQL injection vulnerabilities in SubscriberStart.asp in Active Newsletter 4.3 allow remote attackers to execute arbitrary SQL commands via (1) the email parameter (aka username or E-mail field), or (2) the password parameter (aka password field), to (a) Subscriber.asp or (b) start.asp. NOTE: some of these details are obtained from third party information.	2009-02-25	7.5	CVE-2008-6286 XF MILW0RM SECUNIA
adobe -- acrobat adobe -- acrobat_reader adobe -- reader	Buffer overflow in Adobe Reader 9.0 and earlier and Acrobat 9.0 and earlier allows remote attackers to execute arbitrary code via a crafted PDF document, related to a non-JavaScript function call and possibly an embedded JBIG2 image stream, as exploited in the wild in February 2009 by Trojan.Pidief.E.	2009-02-20	9.3	CVE-2009-0658 CERT CERT-VN XF MISC MISC SECTRACK BID FRSIRT CONFIRM SECUNIA OSVDB MISC
adobe -- air adobe -- flash_player adobe -- flash_player_for_linux adobe -- flex	Unspecified vulnerability in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a crafted Shockwave Flash (aka .swf) file.	2009-02-26	9.3	CVE-2009-0519 BID CONFIRM
adobe -- air adobe -- flash_player	Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 does not properly remove references to destroyed objects during Shockwave Flash file	2009-02-	9.3	CVE-2009-0520 VUPEN

adobe -- flash_player_for_linux adobe -- flex	Shockwave Flash file processing, which allows remote attackers to execute arbitrary code via a crafted file, related to a "buffer overflow issue."	26	9.3	BID CONFIRM MISC
appstate -- phpwebsite	SQL injection vulnerability in links.php in Appalachian State University phpWebSite allows remote attackers to execute arbitrary SQL commands via the cid parameter in a viewlink action.	2009-02-25	7.5	CVE-2008-6266 XF BID BUGTRAQ
aspthai.net -- aspthai.net_webboard	SQL injection vulnerability in bview.asp in ASPThai.Net Webboard 6.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-23	7.5	CVE-2009-0703 XF BID MILW0RM
bluocms -- bluo_cms	SQL injection vulnerability in index.php in Bluo CMS 1.2 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-25	7.5	CVE-2008-6281 BID MILW0RM SECUNIA
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
businessvein -- php_tv_portal	SQL injection vulnerability in index.php in PHP TV Portal 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the mid parameter.	2009-02-25	7.5	CVE-2008-6285 XF VUPEN BID MILW0RM SECUNIA
butterflymedia -- butterfly_organizer	SQL injection vulnerability in view.php in Butterfly Organizer 2.0.1 allows remote attackers to execute arbitrary SQL commands via the mytable parameter. NOTE: the id vector is covered by another CVE name.	2009-02-27	7.5	CVE-2008-6311 MILW0RM SECUNIA
butterflymedia -- butterfly_organizer	SQL injection vulnerability in view.php in Butterfly Organizer 2.0.0 and 2.0.1 allows remote attackers to execute arbitrary SQL commands via the id	2009-02-27	7.5	CVE-2008-6328 MILW0RM MILW0RM SECUNIA

	parameter.			
cafuego -- sdms	SQL injection vulnerability in login.php in Simple Document Management System (SDMS) 1.1.5 and 1.1.4, and possibly earlier, allows remote attackers to execute arbitrary SQL commands via the login parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-21	7.5	CVE-2008-6236 XF BID SECUNIA
cfmsource -- cf_calendar	SQL injection vulnerability in calendarevent.cfm in CF_Calendar allows remote attackers to execute arbitrary SQL commands via the calid parameter.	2009-02-27	7.5	CVE-2008-6319 BID MILW0RM SECUNIA
cfmsource -- cfmblog	SQL injection vulnerability in index.cfm in CFMSource CFMBlog allows remote attackers to execute arbitrary SQL commands via the categorynbr parameter.	2009-02-27	7.5	CVE-2008-6322 BID MILW0RM SECUNIA
cfmsource -- cf_auction	SQL injection vulnerability in forummessages.cfm in CFMSource CF_Auction allows remote attackers to execute arbitrary SQL commands via the categorynbr parameter.	2009-02-27	7.5	CVE-2008-6323 BID MILW0RM
cfmsource -- cf_forum	SQL injection vulnerability in forummessages.cfm in CF_Forum allows remote attackers to execute arbitrary SQL commands via the categorynbr parameter.	2009-02-27	7.5	CVE-2008-6324 BID MILW0RM SECUNIA
cfshopkart -- cf_shopkart	SQL injection vulnerability in index.cfm in CF Shopkart 5.2.2 allows remote attackers to execute arbitrary SQL commands via the Category parameter in a ViewCategory action.	2009-02-27	7.5	CVE-2008-6320 BID MILW0RM SECUNIA
cisco -- meetingplace_web_confrencing	Unspecified vulnerability in the Web Server in Cisco Unified MeetingPlace Web Conferencing 6.0 before 6.0(517.0) (aka 6.0 MR4) and 7.0 before 7.0(2) (aka 7.0 MR1) allows remote attackers to bypass authentication and obtain administrative access via a	2009-02-26	9.0	CVE-2009-0614 BID CISCO

	crafted URL.			
cisco -- application_control_engine_device_manager cisco -- application_networking_manager	Directory traversal vulnerability in Cisco Application Networking Manager (ANM) before 2.0 and Application Control Engine (ACE) Device Manager before A3(2.1) allows remote authenticated users to read or modify arbitrary files via unspecified vectors, related to "invalid directory permissions."	2009-02-26	9.0	CVE-2009-0615 BID CISCO
cisco -- application_networking_manager	Cisco Application Networking Manager (ANM) before 2.0 uses default usernames and passwords, which makes it easier for remote attackers to access the application, or cause a denial of service via configuration changes, related to "default user credentials during installation."	2009-02-26	10.0	CVE-2009-0616 BID CISCO
cisco -- application_networking_manager	Cisco Application Networking Manager (ANM) before 2.0 uses a default MySQL root password, which makes it easier for remote attackers to execute arbitrary operating-system commands or change system files.	2009-02-26	10.0	CVE-2009-0617 BID CISCO
cisco -- application_networking_manager	Unspecified vulnerability in the Java agent in Cisco Application Networking Manager (ANM) before 2.0 Update A allows remote attackers to gain privileges, and cause a denial of service (service outage) by stopping processes, or obtain sensitive information by reading configuration files.	2009-02-26	8.5	CVE-2009-0618 CISCO
cisco -- application_control_engine_module	Cisco ACE Application Control Engine Module for Catalyst 6500 Switches and 7600 Routers before A2(1.1) uses default (1) usernames and (2) passwords for (a) the administrator and (b) web management, which makes it easier for remote attackers to perform configuration	2009-02-26	10.0	CVE-2009-0620 BID CISCO

	changes or obtain operating-system access.			
cisco -- ace_4710	Cisco ACE 4710 Application Control Engine Appliance before A1(8a) uses default (1) usernames and (2) passwords for (a) the administrator, (b) web management, and (c) device management, which makes it easier for remote attackers to perform configuration changes to the Device Manager and other components, or obtain operating-system access.	2009-02-26	10.0	CVE-2009-0621 CISCO
cisco -- ace_4710 cisco -- application_control_engine_module	Unspecified vulnerability in Cisco ACE Application Control Engine Module for Catalyst 6500 Switches and 7600 Routers before A2(1.2) and Cisco ACE 4710 Application Control Engine Appliance before A1(8a) allows remote authenticated users to execute arbitrary operating-system commands through a command line interface (CLI).	2009-02-26	9.0	CVE-2009-0622 CISCO
cisco -- ace_4710 cisco -- application_control_engine_module	Unspecified vulnerability in Cisco ACE Application Control Engine Module for Catalyst 6500 Switches and 7600 Routers before A2(1.3) and Cisco ACE 4710 Application Control Engine Appliance before A3(2.1) allows remote attackers to cause a denial of service (device reload) via a crafted SSH packet.	2009-02-26	7.8	CVE-2009-0623 BID CISCO
cisco -- ace_4710 cisco -- application_control_engine_module	Unspecified vulnerability in Cisco ACE Application Control Engine Module for Catalyst 6500 Switches and 7600 Routers before A2(1.2) and Cisco ACE 4710 Application Control Engine Appliance before A1(8.0) allows remote attackers to cause a denial of service (device reload) via a crafted SNMPv3 packet.	2009-02-26	7.8	CVE-2009-0625 BID CISCO
	The username command in Cisco ACE Application Control Engine Module for			

cisco -- ace_4710 cisco -- application_control_engine_module	Catalyst 6500 Switches and 7600 Routers and Cisco ACE 4710 Application Control Engine Appliance stores a cleartext password by default, which allows context-dependent attackers to obtain sensitive information.	2009-02-26	7.8	CVE-2009-0742 CISCO
craftsilicon -- banking@home	SQL injection vulnerability in Login.asp in Craft Silicon Banking@Home 2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the LoginName parameter.	2009-02-25	7.5	CVE-2009-0741 BID BUGTRAQ SECUNIA FULLDISC
e-topbiz -- admanager	SQL injection vulnerability in view.php in E-topbiz AdManager 4 allows remote attackers to execute arbitrary SQL commands via the group parameter.	2009-02-24	7.5	CVE-2008-6261 XF BID MILW0RM SECUNIA
e-topbiz -- slide_popups	SQL injection vulnerability in admin/admin.php in E-topbiz Slide Popups 1.0 allows remote attackers to execute arbitrary SQL commands via the password parameter.	2009-02-24	7.5	CVE-2008-6264 XF VUPEN BID MISC
e-topbiz -- link_back_checker	E-topbiz Link Back Checker 1 allows remote attackers to bypass authentication and gain administrative access by setting the auth cookie to "admin."	2009-02-26	7.5	CVE-2008-6307 BID MILW0RM SECUNIA OSVDB
emc -- networker_client emc -- networker_module emc -- networker_powersnap emc -- networker_server emc -- networker_storage_node	nsrexecd.exe in multiple EMC Networker products including EMC NetWorker Server, Storage Node, and Client 7.3.x and 7.4, 7.4.1, 7.4.2, Client and Storage Node for Open VMS 7.3.2 ECO6 and earlier, Module for Microsoft Exchange 5.1 and earlier, Module for Microsoft Applications 2.0 and earlier, Module for Meditech 2.0 and earlier, and PowerSnap 2.4 SP1 and earlier does not properly control the allocation of memory, which allows remote attackers to cause a denial of service (memory exhaustion) via multiple crafted RPC requests.	2009-02-20	7.8	CVE-2008-6219 SECTRACK BID BUGTRAQ BUGTRAQ VUPEN MISC 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 VUPEN SECUNIA
frankmancuso -- auth_php	SQL injection vulnerability in login.php in Auth Php 1.0 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) passwd parameters.	2009-02-25	7.5	CVE-2009-0738 BID MILW0RM SECUNIA
frankmancuso -- mynews	SQL injection vulnerability in login.php in MyNews 0.10 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) passwd parameters.	2009-02-25	7.5	CVE-2009-0739 BID MILW0RM
frankmancuso -- bluebird	SQL injection vulnerability in login.php in BlueBird Prelease allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) passwd parameters.	2009-02-25	7.5	CVE-2009-0740 BID MILW0RM
getmiro -- broadcast_machine	Multiple PHP remote file inclusion vulnerabilities in Broadcast Machine 0.1 allow remote attackers to execute arbitrary PHP code via a URL in the baseDir parameter to (1) MySQLController.php, (2) SQLController.php, (3) SetupController.php, (4) VideoController.php, and (5) ViewController.php in controllers/.	2009-02-25	7.5	CVE-2008-6287 XF VUPEN BID MILW0RM
gigcalendar -- gigcalendar_component	SQL injection vulnerability in the GigCalendar (com_gigcal) component 1.0 for Mambo and Joomla! allows remote attackers to execute arbitrary SQL commands via the gigcal_gigs_id parameter in a details action to index.php.	2009-02-24	7.5	CVE-2009-0726 XF BID MILW0RM
gwm -- galatolo_webmanager	SQL injection vulnerability in plugins/users/index.php in Galatolo WebManager 1.3a and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-23	7.5	CVE-2008-6249 BID MILW0RM SECUNIA

gwm -- galatolo_webmanager	Galatolo WebManager 1.3a allows remote attackers to bypass authentication and gain administrative access by setting the (1) gwm_user and (2) gwm_pass cookies to admin. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-26	7.5	CVE-2008-6300 XF MISC BID
hp -- mercury_quality_center hp -- testdirector	HP Mercury Quality Center (QC) 9.2 and earlier, and possibly TestDirector, relies on cached client-side scripts to implement "workflow" and decisions about the "capability" of a user, which allows remote attackers to execute arbitrary code via crafted use of the Open Test Architecture (OTA) API, as demonstrated by modifying (1) common.tds, (2) defects.tds, (3) manrun.tds, (4) req.tds, (5) testlab.tds, or (6) testplan.tds in %tmp%\TD_80, and then setting the file's properties to read-only.	2009-02-24	7.6	CVE-2007-5289 CERT-VN XF BID BUGTRAQ SECUNIA MISC
hp -- virtual_rooms	Unspecified vulnerability in HP Virtual Rooms Client before 7.0.1, when running on Windows, allows remote attackers to execute arbitrary code via unknown vectors.	2009-02-26	7.5	CVE-2009-0208 HP HP
ibm -- websphere_mq	Unspecified vulnerability in the queue manager in IBM WebSphere MQ (WMQ) 5.3, 6.0 before 6.0.2.6, and 7.0 before 7.0.0.2 allows local users to gain privileges via vectors related to the (1) setmqaut, (2) dmpmqaut, and (3) dspmqaut authorization commands.	2009-02-24	7.2	CVE-2009-0439 XF MISC
ibm -- txseries	The CICS listener in IBM TXSeries for Multiplatforms 6.2 GA waits for a forcepurge acknowledgement from the CICS Application Server (CICSAS) after an eci response timeout, which might allow remote authenticated users to cause a denial of service	2009-02-25	9.0	CVE-2009-0505 CONFIRM

	(forcepurge handling delay), or have unspecified other impact, via vectors involving slow or nonexistent acknowledgement.			
infireal -- saturncms	SQL injection vulnerability in lib/url/meta_url.php in SaturnCMS allows remote attackers to execute arbitrary SQL commands via the URL to the translate function. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-24	7.5	CVE-2008-6262 XF SECUNIA
infireal -- saturncms	SQL injection vulnerability in lib/user/t_user.php in SaturnCMS allows remote attackers to execute arbitrary SQL commands via the username parameter to the _userLoggedIn function. NOTE: some of these details are obtained from third party information.	2009-02-24	7.5	CVE-2008-6263 XF BID MILW0RM SECUNIA
interface-medien -- ibase	Directory traversal vulnerability in download.php in Interface Medien ibase 2.03 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter.	2009-02-25	7.8	CVE-2008-6288 XF BID MILW0RM SECUNIA
jadu -- jadu_galaxies	SQL injection vulnerability in scripts/documents.php in Jadu Galaxies allows remote attackers to execute arbitrary SQL commands via the categoryID parameter.	2009-02-24	7.5	CVE-2008-6254 BID MILW0RM SECUNIA
joomla -- com_musica mambo-foundation -- com_musica	SQL injection vulnerability in the com_musica module in Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-02-20	7.5	CVE-2008-6234 BID BUGTRAQ MILW0RM
joovili -- joovili	Joovili 3.1.4 allows remote attackers to bypass authentication and gain privileges as other users, including the administrator, by setting the (1) session_id, session_logged_in, and session_username cookies for user privileges; (2)	2009-02-25	7.5	CVE-2008-6269 XF VUPEN

	session_admin_id, session_admin_username, and session_admin cookies for admin privileges; and (3) session_staff_id, session_staff_username, and session_staff cookies for staff users.	25		BID MILW0RM SECUNIA
libpng -- libpng	Memory leak in the png_handle_tEXt function in pngrutil.c in libpng before 1.2.33 rc02 and 1.4.0 beta36 allows context-dependent attackers to cause a denial of service (memory exhaustion) via a crafted PNG file.	2009-02-20	7.1	CVE-2008-6218 VUPEN CONFIRM CONFIRM
manzovi -- proquiz	SQL injection vulnerability in index.php in ProQuiz 1.0 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-02-27	7.5	CVE-2008-6312 XF BID MILW0RM
manzovi -- proquiz	SQL injection vulnerability in index.php in ProQuiz 1.0 allows remote attackers to execute arbitrary SQL commands via the password parameter, a different vector than CVE-2008-6312.	2009-02-27	7.5	CVE-2008-6327 XF MILW0RM
maran -- php_shop	admin.php in Maran PHP Shop allows remote attackers to bypass authentication and gain administrative access by setting the user cookie to "demo."	2009-02-26	7.5	CVE-2008-6296 XF BID MILW0RM
maxdev -- my_egallery	SQL injection vulnerability in the My_eGallery module for MAXdev MDPro (MD-Pro) and Postnuke allows remote attackers to execute arbitrary SQL commands via the pid parameter in a showpic action to index.php.	2009-02-24	7.5	CVE-2009-0728 BID MILW0RM
microsoft -- excel microsoft -- excel_viewer microsoft -- office microsoft -- office_compatibility_pack microsoft -- office_excel microsoft -- office_excel_viewer	Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP3, and 2007 SP1; Excel Viewer 2003 Gold and SP3; Excel Viewer; Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats SP1; and Excel in Microsoft Office 2004 and 2008 for Mac allow remote attackers to execute arbitrary code via a crafted Excel document that triggers an	2009-02-25	9.3	CVE-2009-0238 XF MISC BID CONFIRM SECTRACK MISC MISC

	access attempt on an invalid object, as exploited in the wild in February 2009 by Trojan.Mdropper.AC.			
miticdjd -- apoll	SQL injection vulnerability in admin/index.php in Dragan Mitic Apoll 0.7 beta and 0.7.5 allows remote attackers to execute arbitrary SQL command via the user parameter.	2009-02-25	7.5	CVE-2008-6270 XF BID MILW0RM
miticdjd -- apoll	SQL injection vulnerability in admin/index.php in Dragan Mitic Apoll 0.7 beta and 0.7.5 allows remote attackers to execute arbitrary SQL command via the pass parameter.	2009-02-25	7.5	CVE-2008-6272 XF 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 VUPEN SECUNIA
nokia -- nokia_pc_suite	Heap-based buffer overflow in MultimediaPlayer.exe 6.86.240.7 in Nokia PC Suite 6.86.9.3 allows remote attackers to execute arbitrary code via a long string in a .m3u playlist file.	2009-02-25	9.3	CVE-2009-0734 VUPEN BUGTRAQ SECUNIA OSVDB
openasp -- openasp	SQL injection vulnerability in default.asp in Openasp 3.0 and earlier allows remote attackers to execute arbitrary SQL commands via the idpage parameter in the pages module.	2009-02-24	7.5	CVE-2008-6257 XF BID MILW0RM SECUNIA
orbitdownloader -- orbit_downloader	Stack-based buffer overflow in Orbit Downloader 2.8.2 and 2.8.3, and possibly other versions before 2.8.5, allows remote attackers to execute arbitrary code via a crafted HTTP URL with a long host name, which is not properly handled when constructing a	2009-02-26	9.3	CVE-2009-0187 VUPEN BID

	"Connecting" log message.			
phoca -- phoca_documentation	SQL injection vulnerability in the Phoca Documentation (com_phocadocumentation) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a section action to index.php.	2009-02-23	7.5	CVE-2009-0702 VUPEN BID MILW0RM
phpfootball -- phpfootball	SQL injection vulnerability in login.php in PHPFootball 1.6 allows remote attackers to execute arbitrary SQL commands via the user parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-23	7.5	CVE-2009-0709 XF SECUNIA OSVDB
phpfootball -- phpfootball	filter.php in PHPFootball 1.6 and earlier allows remote attackers to retrieve password hashes via a request with an Accounts value for the dbtable parameter, in conjunction with a Password value for the dbfield parameter. NOTE: this has been reported as a SQL injection vulnerability by some sources, but the provenance of that information is unknown.	2009-02-23	7.5	CVE-2009-0711 OSVDB MILW0RM SECUNIA
phpmygallery -- phpmygallery	PHP remote file inclusion vulnerability in _conf/core/common-tpl-vars.php in PHPmyGallery 1.0 beta2 allows remote attackers to execute arbitrary PHP code via a URL in the confdir parameter, a different issue than CVE-2008-6316.	2009-02-27	7.5	CVE-2008-6315 BID MILW0RM
phpmygallery -- phpmygallery	PHP remote file inclusion vulnerability in _conf/_php-core/common-tpl-vars.php in PHPmyGallery 1.5 beta allows remote attackers to execute arbitrary PHP code via a URL in the admindir parameter, a different vector than CVE-2008-6317.	2009-02-27	7.5	CVE-2008-6318 BID MILW0RM
	Directory traversal vulnerability in admin.php in			CVE-2009

potato-scripts -- potato_news	Potato News 1.0.0 allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the user cookie parameter.	2009-02-24	7.5	CVE-2009-0722 BID MILW0RM
powerscripts -- powerclan	SQL injection vulnerability in admin/index.php in PowerClan 1.14a allows remote attackers to execute arbitrary SQL commands via the loginemail parameter (aka login field). NOTE: some of these details are obtained from third party information.	2009-02-23	7.5	CVE-2009-0707 XF BID MILW0RM SECUNIA OSVDB
preproject -- pre_multi-vendor_shopping_malls	SQL injection vulnerability in buyer_detail.php in Pre Multi-Vendor Shopping Malls allows remote attackers to execute arbitrary SQL commands via the (1) sid and (2) cid parameters.	2009-02-20	7.5	CVE-2008-6227 BID MILW0RM VUPEN
preproject -- pre_multi-vendor_shopping_malls	Pre Multi-Vendor Shopping Malls allows remote attackers to bypass authentication and gain administrative access by setting the (1) adminname and the (2) adminid cookies to "admin".	2009-02-20	7.5	CVE-2008-6228 MILW0RM VUPEN
preprojects -- 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 VUPEN SECUNIA
preprojects -- pre_classified_listings	Pre Classified Listing PHP allows remote attackers to bypass authentication and gain administrative access by setting the (1) adminname and the (2) adminid cookies to "admin".	2009-02-20	7.5	CVE-2008-6231 MILW0RM VUPEN SECUNIA
preprojects -- pre_shopping_mall	Pre Shopping Mall allows remote attackers to bypass authentication and gain administrative access by setting the (1) adminname and the (2) adminid cookies to "admin".	2009-02-20	7.5	CVE-2008-6232 MILW0RM VUPEN SECUNIA
prezmo -- small_shoutbox	SQL injection vulnerability in shoutbox_view.php in the Small ShoutBox module 1.4 for phpBB allows remote attackers to execute arbitrary SQL commands via the id	2009-02-26	7.5	CVE-2008-6301 BID MILW0RM SECUNIA

	parameter in a delete action.			
quadcomm -- q-shop	SQL injection vulnerability in users.asp in QuadComm Q-Shop 3.0, and possibly earlier, allows remote attackers to execute arbitrary SQL commands via the (1) UserID and (2) Pwd parameters. NOTE: this might be related to CVE-2004-2108.	2009-02-24	7.5	CVE-2008-6258 XF BID MILW0RM SECUNIA
rakhisoftware -- rakhisoftware_shopping_cart	SQL injection vulnerability in product.php in RakhiSoftware Price Comparison Script (aka Shopping Cart) allows remote attackers to execute arbitrary SQL commands via the subcategory_id parameter.	2009-02-25	7.5	CVE-2008-6277 OSVDB MILW0RM SECUNIA MISC
sadi_samami -- multi_languages_webshop_online	SQL injection vulnerability in detail.php in Multi Languages WebShop Online 1.02 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-25	7.5	CVE-2008-6268 BID MILW0RM
scripts-for-sites -- ez_gaming_cheats	SQL injection vulnerability in view_reviews.php in Scripts for Sites (SFS) EZ Gaming Cheats allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-23	7.5	CVE-2008-6244 XF MILW0RM SECUNIA
scripts-for-sites -- ez_biz_pro	SQL injection vulnerability in track.php in Scripts For Sites (SFS) EZ BIZ PRO allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-23	7.5	CVE-2008-6245 XF BID MILW0RM
scripts-for-sites -- ez_webring	SQL injection vulnerability in category.php in Scripts For Sites (SFS) EZ Webring allows remote attackers to execute arbitrary SQL commands via the cat parameter.	2009-02-23	7.5	CVE-2008-6246 XF BID SECUNIA MILW0RM
scripts-for-sites -- ez_top_sites	SQL injection vulnerability in topsite.php in Scripts For Sites (SFS) EZ Top Sites allows remote attackers to execute arbitrary SQL commands via the ts parameter.	2009-02-23	7.5	CVE-2008-6247 XF BID SECUNIA MILW0RM

scripts_for_sites -- hotscripts-like_site	SQL injection vulnerability in software-description.php in Scripts For Sites (SFS) Hotscripts-like Site allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-02-23	7.5	CVE-2008-6237 XF MILW0RM SECUNIA
scripts_for_sites -- ez_e-store	SQL injection vulnerability in SearchResults.php in Scripts For Sites (SFS) EZ e-store allows remote attackers to execute arbitrary SQL commands via the where parameter.	2009-02-23	7.5	CVE-2008-6242 XF BID MILW0RM SECUNIA
scripts_for_sites -- ez_hotscripts-likesite	SQL injection vulnerability in showcategory.php in Scripts For Sites (SFS) Hotscripts-like Site allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-02-23	7.5	CVE-2008-6243 XF MILW0RM SECUNIA
simple-review -- simple_review_component	SQL injection vulnerability in the Simple Review (com_simple_review) component 1.3.5 for Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the category parameter to index.php.	2009-02-23	7.5	CVE-2009-0706 XF BID MISC
simplecustomer -- simple_customer	SQL injection vulnerability in login.php in Simple Customer as downloaded on 20081118 allows remote attackers to execute arbitrary SQL commands via the email parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-27	7.5	CVE-2008-6326 XF OSVDB SECUNIA
smcfancontrol -- smcfancontrol	Stack-based buffer overflow in the smc program in smcFanControl 2.1.2 allows local users to execute arbitrary code and gain privileges via a long -k option.	2009-02-24	7.2	CVE-2008-6252 VUPEN CONFIRM
tony_iha_kazungu -- taifajobs	SQL injection vulnerability in jobdetails.php in taifajobs 1.0 and earlier allows remote attackers to execute arbitrary SQL commands via the jobid parameter.	2009-02-24	7.5	CVE-2009-0727 BID BUGTRAQ MILW0RM MISC
	SQL injection vulnerability in cityview.php in Tours			CVE-2008-6289

toursmanager -- tours_manager	Manager 1.0 allows remote attackers to execute arbitrary SQL commands via the cityid parameter.	2009-02-26	7.5	6289 BID MILW0RM SECUNIA
toursmanager -- tours_manager	SQL injection vulnerability in tourview.php in ToursManager allows remote attackers to execute arbitrary SQL commands via the tourid parameter.	2009-02-26	7.5	CVE-2008-6303 BID MILW0RM SECUNIA
turnkeyforms -- local_classifieds	TurnkeyForms Local Classifieds allows remote attackers to bypass authentication and gain administrative access via a direct request to Site_Admin/admin.php.	2009-02-26	7.5	CVE-2008-6302 MILW0RM SECUNIA
ultrastats -- ultrastats	SQL injection vulnerability in index.php in Ultrastats 0.2.144 and 0.3.11 allows remote attackers to execute arbitrary SQL commands via the serverid parameter.	2009-02-24	7.5	CVE-2008-6260 BID MILW0RM SECUNIA
vim -- tar.vim vim -- vim	The shellescape function in Vim 7.0 through 7.2, including 7.2a.10, allows user-assisted attackers to execute arbitrary code via the "!" (exclamation point) shell metacharacter in (1) the filename of a tar archive and possibly (2) the filename of the first file in a tar archive, which is not properly handled by the VIM TAR plugin (tar.vim) v.10 through v.22, as demonstrated by the shellescape, tarplugin.v2, tarplugin, and tarplugin.updated test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712. NOTE: this issue has the same root cause as CVE-2008-3075. NOTE: due to the complexity of the associated disclosures and the incomplete information related to them, there may be inaccuracies in this CVE description and in external mappings to this identifier.	2009-02-21	9.3	CVE-2008-3074 MISC MLIST
	The shellescape function in Vim 7.0 through 7.2, including 7.2a.10, allows			

vim -- vim vim -- zipplugin.vim	user-assisted attackers to execute arbitrary code via the "!" (exclamation point) shell metacharacter in (1) the filename of a ZIP archive and possibly (2) the filename of the first file in a ZIP archive, which is not properly handled by zip.vim in the VIM ZIP plugin (zipPlugin.vim) v.11 through v.21, as demonstrated by the zipplugin and zipplugin.v2 test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712. NOTE: this issue has the same root cause as CVE-2008-3074. NOTE: due to the complexity of the associated disclosures and the incomplete information related to them, there may be inaccuracies in this CVE description and in external mappings to this identifier.	2009-02-21	9.3	CVE-2008-3075 MISC MLIST
vim -- vim	The Netrw plugin 125 in netrw.vim in Vim 7.2a.10 allows user-assisted attackers to execute arbitrary code via shell metacharacters in filenames used by the execute and system functions within the (1) mz and (2) mc commands, as demonstrated by the netrw.v2 and netrw.v3 test cases. NOTE: this issue reportedly exists because of an incomplete fix for CVE-2008-2712.	2009-02-21	9.3	CVE-2008-3076 MISC MISC MLIST
vim -- vim	The Netrw plugin (netrw.vim) in Vim 7.0 and 7.1 allows user-assisted attackers to execute arbitrary commands via shell metacharacters in a filename used by the (1) "D" (delete) command or (2) b:netrw_curdir variable, as demonstrated using the netrw.v4 and netrw.v5 test cases.	2009-02-21	9.3	CVE-2008-6235 MISC MISC
	SQL injection vulnerability in index.php in W3matter AskPert allows remote attackers to execute arbitrary	2009-02		CVE-2008-6309

w3matter -- askpert	SQL commands via the f[password] parameter. NOTE: some of these details are obtained from third party information.	2009-02-26	7.5	BID MILW0RM SECUNIA
w3matter -- revsense	SQL injection vulnerability in index.php in W3matter RevSense 1.0 allows remote attackers to execute arbitrary SQL commands via the f[password] parameter. NOTE: some of these details are obtained from third party information.	2009-02-26	7.5	CVE-2008-6310 BID MILW0RM SECUNIA
webmastersite -- wsn_guest	SQL injection vulnerability in search.php in WSN Guest 1.23 allows remote attackers to execute arbitrary SQL commands via the search parameter in an advanced action.	2009-02-23	7.5	CVE-2009-0704 XF BID MILW0RM
wotw -- way_of_the_warrior	PHP remote file inclusion vulnerability in visualizza.php in Way Of The Warrior (WOTW) 5.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the plancia parameter to crea.php.	2009-02-20	7.5	CVE-2008-6223 XF BID SECUNIA MILW0RM
xine -- xine-lib	Integer overflow in the 4xm demuxer (demuxers/demux_4xm.c) in xine-lib 1.1.16.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a 4X movie file with a large current_track value, a similar issue to CVE-2009-0385.	2009-02-23	7.5	CVE-2009-0698 CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- air adobe -- flash_player adobe -- flash_player_for_linux adobe -- flex	Unspecified vulnerability in the Settings Manager in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87, and possibly other versions, allows remote attackers to trick a user into visiting an arbitrary URL via unknown vectors, related to "a potential Clickjacking issue variant."	2009-02-26	5.8	CVE-2009-0114 VUPEN CONFIRM
adobe -- flash_player_for_linux	Untrusted search path vulnerability in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 on Linux allows local users to obtain sensitive information or gain privileges via a crafted library in a directory contained in the RPATH.	2009-02-26	4.6	CVE-2009-0521 VUPEN CONFIRM

adobe -- air adobe -- flash_player adobe -- flash_player_for_linux adobe -- flex	Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 on Windows allows remote attackers to trick a user into visiting an arbitrary URL via an unspecified manipulation of the "mouse pointer display," related to a "Clickjacking attack."	2009-02-26	4.3	CVE-2009-0522 CONFIRM
adobe -- robohelp adobe -- robohelp_server	Cross-site scripting (XSS) vulnerability in Adobe RoboHelp Server 6 and 7 allows remote attackers to inject arbitrary web script or HTML via a crafted URL, which is not properly handled when displaying the Help Errors log.	2009-02-26	4.3	CVE-2009-0523 VUPEN BID CONFIRM
adobe -- robohelp adobe -- robohelp_server	Cross-site scripting (XSS) vulnerability in Adobe RoboHelp 6 and 7, and RoboHelp Server 6 and 7, allows remote attackers to inject arbitrary web script or HTML via vectors involving files produced by RoboHelp.	2009-02-26	4.3	CVE-2009-0524 BID CONFIRM
apache -- tomcat	The doRead method in Apache Tomcat 4.1.32 through 4.1.34 and 5.5.10 through 5.5.20 does not return a -1 to indicate when a certain error condition has occurred, which can cause Tomcat to send POST content from one request to a different request.	2009-02-26	5.0	CVE-2008-4308 VUPEN
asus -- smartlogon	Asus SmartLogon 1.0.0005 allows physically proximate attackers to bypass "security functions" by presenting an image with a modified viewpoint that matches the posture of a stored image of the authorized notebook user.	2009-02-20	6.9	CVE-2009-0656 MISC MISC
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
camera_life -- camera_life	Multiple cross-site scripting (XSS) vulnerabilities in Camera Life 2.6.2b8 allow remote attackers to inject arbitrary web script or HTML via the q parameter to (1) search.php and (2) rss.php; the query string after the image name in (3) photos/photo; the path parameter to (4) folder.php; page parameter and REQUEST_URI to (5) login.php; ver parameter to (6) media.php; theme parameter to (7) modules/iconset/iconset-debug.php; and the REQUEST_URI to (8) index.php.	2009-02-26	4.3	CVE-2008-6295 XF BID MISC SECUNIA
cfshopkart -- cf_shopkart	CF Shopkart 5.2.2 stores cfshopkart52.mdb under the web root with insufficient access control, which allows remote attackers to obtain sensitive information, such as usernames and passwords, via a direct request.	2009-02-27	5.0	CVE-2008-6321 MILW0RM SECUNIA
china-on-site -- flexphpsite	Multiple SQL injection vulnerabilities in admin/usercheck.php in FlexPHPSite 0.0.1 and 0.0.7, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via (1) the checkuser parameter (aka username field), or (2) the checkpass parameter (aka password field), to admin/index.php.	2009-02-23	6.8	CVE-2008-6241 XF MILW0RM SECUNIA
cisco -- wrt160n	Cross-site scripting (XSS) vulnerability in apply.cgi on the Linksys WRT160N allows remote attackers to inject arbitrary web script or HTML via the action parameter in a DHCP_Static operation.	2009-02-25	4.3	CVE-2008-6280 BID SECUNIA MISC
cisco -- ace_4710 cisco -- application_control_engine_module	Unspecified vulnerability in the SNMPv2c implementation in Cisco ACE Application Control Engine Module for Catalyst 6500 Switches and 7600 Routers before A2(1.3) and Cisco ACE 4710 Application Control Engine Appliance before A3(2.1) allows remote attackers to cause a denial of service (device reload) via a crafted SNMPv1 packet.	2009-02-26	6.8	CVE-2009-0624 CISCO

comdev -- comdev_web_blogger	SQL injection vulnerability in Comdev Web Blogger 4.1.3 and earlier allows remote attackers to execute arbitrary SQL commands via the arcmonth parameter to a blog page.	2009-02-23	6.8	CVE-2008-6250 BID BUGTRAQ MILW0RM SECUNIA MISC
cyberfolio -- cyberfolio	Directory traversal vulnerability in portfolio/css.php in Cyberfolio 7.12.2 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the theme parameter.	2009-02-24	6.8	CVE-2008-6265 XF VUPEN BID MILW0RM
cybershade -- cybershadecms	Multiple PHP remote file inclusion vulnerabilities in index.php in Cybershade CMS 0.2b, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) THEME_header and (2) THEME_footer parameters.	2009-02-23	6.8	CVE-2009-0701 XF BID MILW0RM
dhcart -- dhcart	Cross-site scripting (XSS) vulnerability in order.php in DHCart allows remote attackers to inject arbitrary web script or HTML via the (1) domain and (2) d1 parameters.	2009-02-26	4.3	CVE-2008-6297 SECUNIA 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 XF MILW0RM VUPEN SECUNIA OSVDB
dmitry_baryshev -- ksquirrel-libs	Multiple stack-based buffer overflows in the mt_codec::getHdrHead function in kernel/kls_hdr/fmt_codec_hdr.cpp in ksquirrel-libs 0.8.0 allow context-dependent attackers to execute arbitrary code via a crafted Radiance RGBE image (aka .hdr file).	2009-02-26	6.8	CVE-2008-5263 XF VUPEN BID BUGTRAQ MISC SECUNIA
drupal -- user_karma_module	Multiple SQL injection vulnerabilities in the User Karma module 5.x before 5.x-1.13 and 6.x before 6.x-1.0-beta1, a module for Drupal, allow remote authenticated administrators to execute arbitrary SQL commands via (1) a content type or (2) a voting API value.	2009-02-25	6.5	CVE-2008-6276 BID CONFIRM
freedirectoryscript -- free_directory_script	PHP remote file inclusion vulnerability in init.php in Free Directory Script 1.1.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the API_HOME_DIR parameter.	2009-02-26	6.8	CVE-2008-6305 XF MILW0RM SECUNIA OSVDB
galatolo -- galatolo_webmanager	Cross-site scripting (XSS) vulnerability in all.php in Galatolo WebManager 1.3a and earlier allows remote attackers to inject arbitrary web script or HTML via the tag parameter.	2009-02-23	4.3	CVE-2008-6248 XF BID MILW0RM SECUNIA
	Multiple SQL injection vulnerabilities in the GigCalendar			CVE-2009

gigcalendar -- gigcalendar_component	(com_gigcal) component 1.0 for Mambo and Joomla!, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via (1) the gigcal _venues_id parameter in a details action to index.php, which is not properly handled by venuedetails.php, and (2) the gigcal_bands_id parameter in a details action to index.php, which is not properly handled by banddetails.php, different vectors than CVE-2009-0726.	2009-02-24	6.8	CVE-2009-0730 XF BID BID BUGTRAQ BUGTRAQ BUGTRAQ
ibm -- websphere_application_server	Unspecified vulnerability in IBM WebSphere Application Server (WAS) 5.1 and 6.0.2 before 6.0.2.33 on z/OS, when CSIv2 Identity Assertion is enabled and Enterprise JavaBeans (EJB) interaction occurs between a WAS 6.1 instance and a WAS pre-6.1 instance, allows local users to have an unknown impact via vectors related to (1) use of the wrong subject and (2) multiple CBIND checks.	2009-02-25	6.2	CVE-2009-0506 XF CONFIRM
ibm -- websphere_process_server	IBM WebSphere Process Server (WPS) 6.1.2 before 6.1.2.3 and 6.2 before 6.2.1.0 does not properly restrict configuration data during an export of the cluster configuration file from the administrative console, which allows remote authenticated users to obtain (1) JMSAPI information and (2) mail session information via vectors involving access to a cluster member.	2009-02-26	4.0	CVE-2009-0507 XF AIXAPAR
insightinformatics -- libero	Cross-site scripting (XSS) vulnerability in Libero 5.3 SP5, and possibly other versions before 5.5 SP1, allows remote attackers to inject arbitrary web script or HTML via the search term field.	2009-02-25	4.3	CVE-2009-0540 XF VUPEN BID FULLDISC
libpng -- libpng	The PNG reference library (aka libpng) before 1.0.43, and 1.2.x before 1.2.35, as used in pngcrush and other applications, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file that triggers a free of an uninitialized pointer in (1) the png_read_png function, (2) pCAL chunk handling, or (3) setup of 16-bit gamma tables.	2009-02-22	6.8	CVE-2009-0040 VUPEN
lingx -- page_engine_cms	Multiple directory traversal vulnerabilities in Page Engine CMS 2.0 Basic and Pro allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the fPrefix parameter to (1) modules/recent_poll_include.php, (2) modules/login_include.php, and (3) modules/statistics_include.php and (4) configuration.inc.php in includes/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-24	6.8	CVE-2009-0729 XF BID SECUNIA OSVDB OSVDB OSVDB OSVDB
lingx -- downloadcenter	Downloadcenter 2.1 stores common.h under the web root with insufficient access control, which allows remote attackers to obtain user credentials and other sensitive information via a direct request. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-24	5.0	CVE-2009-0732 XF SECUNIA OSVDB
magentocommerc -- magento	Multiple cross-site scripting (XSS) vulnerabilities in Magento 1.2.0 and 1.2.1.1 allow remote attackers to inject arbitrary web script or HTML via (1) the username field in an admin/ request to index.php, possibly related to the login[username] parameter and the app/code/core/Mage/Admin/Model/Session.php login function; (2) the email address field in an admin/index/forgotpassword/ request to index.php, possibly	2009-02-25	4.3	CVE-2009-0541 XF XF XF BID

	related to the email parameter and the app/code/core/Mage/Adminhtml/controllers/IndexController.php forgotpasswordAction function; or (3) the return parameter to the default URI under downloader/.			SECTRACK SECUNIA FULLDISC
mjcreation -- familyproject	Multiple SQL injection vulnerabilities in index.php in FamilyProject 2.0 allow remote attackers to execute arbitrary SQL commands via (1) the logmbr parameter (aka login field) or (2) the mdpmbr parameter (aka pass or "Mot de passe" field). NOTE: some of these details are obtained from third party information.	2009-02-25	6.8	CVE-2008-6274 MILW0RM SECUNIA OSVDB
myktools -- myktools	Directory traversal vulnerability in configuration_script.php in MyKtools 3.0 allows remote authenticated administrators to include and execute arbitrary local files via a .. (dot dot) in the langage parameter, a different vulnerability than CVE-2008-4781. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-25	6.0	CVE-2008-6273 SECUNIA
niclor -- include_sito	Directory traversal vulnerability in includefile.php in nicLOR Sito, when register_globals is enabled or magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the page_file parameter.	2009-02-26	6.8	CVE-2008-6290 MILW0RM SECUNIA
openedit -- openedit_digital_asset_management	Cross-site request forgery (CSRF) vulnerability in OpenEdit Digital Asset Management (DAM) before 5.2014 allows remote attackers to perform unspecified actions as arbitrary users via unknown vectors.	2009-02-23	4.3	CVE-2008-6239 XF OSVDB SECUNIA MISC
openedit -- openedit_digital_asset_management	Cross-site scripting (XSS) vulnerability in data/views/index.html in OpenEdit Digital Asset Management (DAM) before 5.2014 allows remote attackers to inject arbitrary web script or HTML via the catalogid parameter.	2009-02-23	4.3	CVE-2008-6240 XF BID OSVDB SECUNIA MISC
ortus.nirn -- cms_ortus	SQL injection vulnerability in engine/users/users_edit_pub.inc in CMS Ortus 1.13 and earlier allows remote authenticated users to execute arbitrary SQL commands via the city parameter in a users_edit_pub action to index.php.	2009-02-25	6.5	CVE-2008-6282 CONFIRM
papoo -- papoo	Directory traversal vulnerability in lib/classes/message_class.php in Papoo CMS 3.6, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to read and possibly execute arbitrary files via a .. (dot dot) in the pfadhier parameter. NOTE: some of these details are obtained from third party information.	2009-02-25	5.1	CVE-2009-0735 BID MILW0RM SECUNIA
phpaddedit -- phpaddedit	Directory traversal vulnerability in addedit-render.php in phpAddEdit 1.3, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a URL in the editform parameter. NOTE: PHP remote file inclusion attacks are also likely.	2009-02-27	6.8	CVE-2008-6313 BID MILW0RM SECUNIA
phpfootball -- phpfootball	Multiple cross-site scripting (XSS) vulnerabilities in PHPFootball 1.6 allow remote attackers to inject arbitrary web script or HTML via (1) the user parameter to login.php or (2) the dbfield parameter to filter.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-23	4.3	CVE-2009-0710 XF XF OSVDB SECUNIA OSVDB

phpmygallery -- phpmygallery	Directory traversal vulnerability in _conf/core/common-tpl-vars.php in PHPmyGallery 1.0 beta2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter, a different issue than CVE-2008-6316 and a different vector than CVE-2008-6318.	2009-02-27	6.8	CVE-2008-6316 XF BID MILW0RM
phpmygallery -- phpmygallery	Directory traversal vulnerability in _conf/_php-core/common-tpl-vars.php in PHPmyGallery 1.5 beta allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the conf[lang] parameter, a different issue than CVE-2008-6318. NOTE: this might be the same issue as CVE-2008-6316.	2009-02-27	6.8	CVE-2008-6317 XF BID MILW0RM
pluck-cms -- pluck	Directory traversal vulnerability in data/inc/lib/pcltar.lib.php in Pluck 4.5.3, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the g_pcltar_lib_dir parameter.	2009-02-24	6.8	CVE-2008-6253 BID BUGTRAQ CONFIRM SECUNIA
plunet -- business_manager	Plunet BusinessManager 4.1 and earlier allows remote authenticated users to bypass access restrictions and (1) read sensitive Customer or Order data via a modified Pfad parameter to pagesUTF8/Sys_DirAnzeige.jsp, or (2) list sensitive Jobs via a direct request to pagesUTF8/auftrag_job.jsp.	2009-02-23	5.5	CVE-2009-0700 XF BID MISC BUGTRAQ BUGTRAQ
powerscripts -- powernews	SQL injection vulnerability in news.php in PowerScripts PowerNews 2.5.4, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the newsid parameter.	2009-02-23	6.8	CVE-2009-0705 XF BID MILW0RM SECUNIA OSVDB
punbb -- private_messaging_system	Multiple directory traversal vulnerabilities in Private Messaging System (PMS) 1.2.3 and earlier for PunBB allow remote attackers to include and execute arbitrary files via a .. (dot dot) in the pun_user[language] parameter to (1) functions_navlinks.php, (2) header_new_messages.php, (3) profile_send.php, and (4) viewtopic_PM-link.php in include/pms/.	2009-02-26	5.1	CVE-2008-6308 VUPEN BID MILW0RM SECUNIA
quadcomm -- q-shop	Cross-site scripting (XSS) vulnerability in search.asp in QuadComm Q-Shop 3.0, and possibly earlier, allows remote attackers to inject arbitrary web script or HTML via the srkeys parameter.	2009-02-24	4.3	CVE-2008-6259 XF BID MILW0RM SECUNIA
rakhisoftware -- rakhisoftware_shopping_cart	Multiple cross-site scripting (XSS) vulnerabilities in product.php in RakhiSoftware Price Comparison Script (aka Shopping Cart) allow remote attackers to inject arbitrary web script or HTML via the (1) category_id and (2) subcategory_id parameters.	2009-02-25	4.3	CVE-2008-6278 BID SECUNIA MISC OSVDB
rakhisoftware -- rakhisoftware_shopping_cart	RakhiSoftware Price Comparison Script (aka Shopping Cart) allows remote attackers to obtain sensitive information via an invalid PHPSESSID cookie, which reveals the installation path in an error message.	2009-02-25	5.0	CVE-2008-6279 BID SECUNIA MISC OSVDB

ravenphpscripts -- ravennuke	SQL injection vulnerability in the Resend_Email module in Raven Web Services RavenNuke 2.30 allows remote authenticated administrators to execute arbitrary SQL commands via the user_prefix parameter to modules.php.	2009-02-22	6.5	CVE-2009-0672 BID
ravenphpscripts -- ravennuke	Eval injection vulnerability in the Custom Fields feature in the Your Account module in Raven Web Services RavenNuke 2.30 allows remote authenticated administrators to execute arbitrary PHP code via the ID Field Name box in a yaCustomFields action to admin.php.	2009-02-22	6.5	CVE-2009-0673 XF MISC BID BUGTRAQ MILW0RM CONFIRM
rocketeer.dip -- sisapilocation	Unspecified vulnerability in sISAPILocation before 1.0.2.2 allows remote attackers to bypass intended access restrictions for character encoding and the cookie secure flag via unknown vectors related to the "HTTP header rewrite function."	2009-02-26	5.0	CVE-2008-6298 CONFIRM
sadi_samami -- multi_languages_webshop_online	Cross-site scripting (XSS) vulnerability in detail.php in Multi Languages WebShop Online 1.02 allows remote attackers to inject arbitrary web script or HTML via the name parameter.	2009-02-25	4.3	CVE-2008-6267 BID MILW0RM
scripts -- phpfan	PHP remote file inclusion vulnerability in includes/init.php in phpFan 3.3.4 allows remote attackers to execute arbitrary PHP code via a URL in the includepath parameter.	2009-02-24	6.8	CVE-2008-6251 CONFIRM
semanticscuttle -- semanticscuttle	Multiple cross-site request forgery (CSRF) vulnerabilities in SemanticScuttle before 0.91 allow remote attackers to perform (1) unspecified actions as administrators via unknown vectors or (2) unspecified actions as arbitrary users via vectors involving the profile page.	2009-02-23	6.8	CVE-2009-0708 CONFIRM
simon_brown -- pebble	Cross-site scripting (XSS) vulnerability in Pebble before 2.3.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-02-25	4.3	CVE-2009-0736 CONFIRM CONFIRM
softbizscripts -- classifieds_script	Cross-site scripting (XSS) vulnerability in signinform.php in Softbiz Classifieds Script allows remote attackers to inject arbitrary web script or HTML via the msg parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-02-26	4.3	CVE-2008-6306 XF BID SECUNIA
softbizscripts -- classifieds_script	Multiple cross-site scripting (XSS) vulnerabilities in Softbiz Classifieds Script allow remote attackers to inject arbitrary web script or HTML via the (1) radio parameter to showcategory.php, (2) msg parameter to advertisers/signinform.php, (3) radio parameter to gallery.php, (4) msg parameter to lostpassword.php, (5) radio parameter to showcategory.php, (6) msg parameter to admin/adminhome.php, and (7) msg parameter to admin/index.php. NOTE: a different signinform.php file is already covered by CVE-2008-6306.	2009-02-27	4.3	CVE-2008-6325 SECUNIA MISC
subtextproject -- subtext	Cross-site scripting (XSS) vulnerability in Subtext 2.0 allows remote attackers to inject arbitrary web script or HTML via a comment, related to "the feature which converts URLs to anchor tags."	2009-02-25	4.3	CVE-2008-6283 BID CONFIRM MISC
tbmnet -- tbmnetcms	Directory traversal vulnerability in index.php in TBmnetCMS 1.0, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the content	2009-02-25	6.8	CVE-2008-6271 BID MILW0RM

	parameter.			MILWORM SECUNIA
tor -- tor	Tor 0.2.0.28, and probably 0.2.0.34 and earlier, allows remote attackers, with control of an entry router and an exit router, to confirm that a sender and receiver are communicating via vectors involving (1) replaying, (2) modifying, (3) inserting, or (4) deleting a single cell, and then observing cell recognition errors at the exit router. NOTE: the vendor disputes the significance of this issue, noting that the product's design "accepted end-to-end correlation as an attack that is too expensive to solve."	2009-02-20	5.1	CVE-2009-0654 MISC MISC MISC
vbulletin -- vbulletin	Multiple SQL injection vulnerabilities in vBulletin 3.7.4 allow remote authenticated administrators to execute arbitrary SQL commands via the (1) answer parameter to admincp/verify.php, (2) extension parameter in an edit action to admincp/attachmentpermission.php, and the (3) iperm parameter to admincp/image.php.	2009-02-24	6.5	CVE-2008-6255 MISC BUGTRAQ SECUNIA
vbulletin -- vbulletin	SQL injection vulnerability in admincp/admincalendar.php in vBulletin 3.7.3.pl1 allows remote authenticated administrators to execute arbitrary SQL commands via the holidayinfo[recurring] parameter, a different vector than CVE-2005-3022.	2009-02-24	6.5	CVE-2008-6256 MISC BUGTRAQ SECUNIA
xt-commerce -- xt-commerce	SQL injection vulnerability in xt:Commerce before 3.0.4 Sp2.1, when magic_quotes_gpc is enabled and the SEO URLs are activated, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-02-26	6.8	CVE-2008-6304 CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
drupal -- content_construction_kit	Cross-site scripting (XSS) vulnerability in the administrative interface in Drupal Content Construction Kit (CCK) 5.x before 5.x-1.10 and 6.x before 6.x-2.0, a module for Drupal, allows remote authenticated users with "administer content" permissions to inject arbitrary web script or HTML via (1) field labels and (2) content-type names.	2009-02-20	3.5	CVE-2008-6229 BID CONFIRM
drupal -- user_karma_module	Cross-site scripting (XSS) vulnerability in the User Karma module 5.x before 5.x-1.13 and 6.x before 6.x-1.0-beta1, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified messages.	2009-02-25	1.9	CVE-2008-6275 BID CONFIRM
joomla -- joomla	Multiple cross-site scripting (XSS) vulnerabilities in Joomla! 1.5.7 and earlier allow remote authenticated users with certain privileges to inject arbitrary web script or HTML via (1) the title and description parameters to the com_weblinks module and (2) unspecified vectors in the com_content module related to "article submission."	2009-02-26	3.5	CVE-2008-6299 CONFIRM CONFIRM
	The skfp_ioctl function in drivers/net/skfp/skfddi.c in the Linux kernel before 2.6.28.6 permits SKFP_CLR_STATS			CVE-2009-0675 CONFIRM

linux -- kernel	requests only when the CAP_NET_ADMIN capability is absent, instead of when this capability is present, which allows local users to reset the driver statistics, related to an "inverted logic" issue.	2009-02-22	2.1	CONFIRM SECUNIA MLIST MLIST CONFIRM
linux -- kernel	The sock_getsockopt function in net/core/sock.c in the Linux kernel before 2.6.28.6 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel memory via an SO_BSDCOMPAT getsockopt request.	2009-02-22	2.1	CVE-2009-0676 BID
mediawiki -- mediawiki	Multiple cross-site scripting (XSS) vulnerabilities in the web-based installer (config/index.php) in MediaWiki 1.6 before 1.6.12, 1.12 before 1.12.4, and 1.13 before 1.13.4, when the installer is in active use, allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-02-25	2.6	CVE-2009-0737 VUPEN BID MLIST
plunet -- business_manager	Cross-site scripting (XSS) vulnerability in pagesUTF8/auftrag_allgemeinauftrag.jsp in Plunet BusinessManager 4.1 and earlier allows remote authenticated users to inject arbitrary web script or HTML via the (1) QUB and (2) Bez74 parameters.	2009-02-23	3.5	CVE-2009-0699 XF BID MISC BUGTRAQ BUGTRAQ

Back to top