The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
activewebsoftwares -- active_trade	SQL injection vulnerability in account.asp in Active Trade 2 allows remote attackers to execute arbitrary SQL commands via the (1) username parameter (aka Email field) or the (2) password parameter. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5627 MILW0RM SECUNIA
activewebsoftwares -- active_ewebquiz	SQL injection vulnerability in start.asp in Active eWebquiz 8.0 allows remote attackers to execute arbitrary SQL commands via the (1) useremail parameter (aka username field) or the (2) password parameter. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5631 MILW0RM SECUNIA
activewebsoftwares -- active_time_billing	SQL injection vulnerability in Account.asp in Active Time Billing 3.2 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters, possibly related to start.asp. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5632 MILW0RM FRSIRT SECUNIA
activewebsoftwares -- activevotes	SQL injection vulnerability in register.asp in ActiveVotes 2.2 allows remote attackers to execute arbitrary SQL commands via the (1)	2008-12-17	7.5	CVE-2008-5633 MILW0RM SECUNIA
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	username and (2) password parameters, possibly related to start.asp. NOTE: some of these details are obtained from third party information.			
activewebsoftwares -- active_force_matrix	SQL injection vulnerability in account.asp in Active Force Matrix 2.0 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters, possibly related to start.asp. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5634 MILW0RM SECUNIA
activewebsoftwares -- active_membership	SQL injection vulnerability in account.asp in Active Membership 2.0 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters, possibly related to start.asp. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5635 MILW0RM SECUNIA
activewebsoftwares -- active_price_comparison	Multiple SQL injection vulnerabilities in Active Price Comparison 4 allow remote attackers to execute arbitrary SQL commands via the (1) ProductID parameter to reviews.aspx or the (2) linkid parameter to links.asp.	2008-12-17	7.5	CVE-2008-5638 MILW0RM SECUNIA
activewebsoftwares -- active_bids	SQL injection vulnerability in bidhistory.asp in Active Bids 3.5 allows remote attackers to execute arbitrary SQL commands via the ItemID parameter.	2008-12-17	7.5	CVE-2008-5640 MILW0RM FRSIRT SECUNIA
activewebsoftwares -- active_photo_gallery	SQL injection vulnerability in account.asp in Active Photo Gallery 6.2 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password parameters.	2008-12-17	7.5	CVE-2008-5641 MILW0RM FRSIRT SECUNIA
adcomplete -- poll_pro	SQL injection vulnerability in the login feature in Poll Pro 2.0 allows remote attackers to execute arbitrary SQL commands via the (1) Password and (2) username parameters.	2008-12-15	7.5	CVE-2008-5573 BID MILW0RM SECUNIA OSVDB
adobe -- flash_playe_for_linux adobe -- flash_player_for_linux	Unspecified vulnerability in Adobe Flash Player for Linux 10.0.12.36, and 9.0.151.0 and earlier, allows remote attackers to execute arbitrary code via a crafted SWF file.	2008-12-17	9.3	CVE-2008-5499 CONFIRM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
alstrasoft -- article_manager_pro	SQL injection vulnerability in admin/admin.php in AlstraSoft Article Manager Pro 1.6 allows remote attackers to execute arbitrary SQL commands via the username parameter.	2008-12-17	10.0	CVE-2008-5649 BID MILW0RM FRSIRT SECUNIA
alstrasoft -- webhost_directory	SQL injection vulnerability in the login directory in AlstraSoft Web Host Directory allows remote attackers to execute arbitrary SQL commands via the pwd parameter.	2008-12-17	7.5	CVE-2008-5650 MILW0RM SECUNIA
apple -- mac_os_x apple -- mac_os_x_server	Integer signedness error in BOM in Apple Mac OS X before 10.5.6 allows remote attackers to execute arbitrary code via the headers in a crafted CPIO archive, leading to a stack-based buffer overflow.	2008-12-16	9.3	CVE-2008-4217 CERT BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Multiple integer overflows in the kernel in Apple Mac OS X before 10.5.6 on Intel platforms allow local users to gain privileges via a crafted call to (1) i386_set_ldt or (2) i386_get_ldt.	2008-12-16	7.2	CVE-2008-4218 CERT BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Integer overflow in the inet_net_pton API in Libsystem in Apple Mac OS X before 10.5.6 allows context-dependent attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors. NOTE: this may be related to the WLB-2008080064 advisory published by SecurityReason on 20080822; however, as of 20081216, there are insufficient details to be sure.	2008-12-16	10.0	CVE-2008-4220 CERT BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	The strptime API in Libsystem in Apple Mac OS X before 10.5.6 allows context-dependent attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via a crafted date string, related to improper memory allocation.	2008-12-16	10.0	CVE-2008-4221 CERT BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	natd in network_cmds in Apple Mac OS X before 10.5.6, when Internet Sharing is enabled, allows remote attackers to cause a denial of service (infinite loop) via a crafted TCP packet.	2008-12-16	7.1	CVE-2008-4222 CERT BID CONFIRM SECUNIA APPLE

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
apple -- mac_os_x_server	Podcast Producer in Apple Mac OS X 10.5 before 10.5.6 allows remote attackers to bypass authentication and gain administrative access via unspecified vectors.	2008-12-16	10.0	CVE-2008-4223 CERT SECTRACK BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	UDF in Apple Mac OS X before 10.5.6 allows user-assisted attackers to cause a denial of service (system crash) via a malformed UDF volume in a crafted ISO file.	2008-12-16	7.1	CVE-2008-4224 CERT SECTRACK BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Incomplete blacklist vulnerability in the Quarantine feature in CoreTypes in Apple Mac OS X 10.5 before 10.5.6 allows user-assisted remote attackers to execute arbitrary code via an executable file with the content type indicating no application association for the file, which does not trigger a "potentially unsafe" warning message.	2008-12-16	9.3	CVE-2008-4234 CERT SECTRACK BID CONFIRM SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Apple Type Services (ATS) in Apple Mac OS X 10.5 before 10.5.6 allows remote attackers to cause a denial of service (infinite loop) via a crafted embedded font in a PDF file.	2008-12-16	7.1	CVE-2008-4236 CERT BID CONFIRM SECTRACK SECUNIA APPLE
apple -- mac_os_x apple -- mac_os_x_server	Managed Client in Apple Mac OS X before 10.5.6 sometimes misidentifies a system when installing per-host configuration settings, which allows context-dependent attackers to have an unspecified impact by leveraging unintended settings, as demonstrated by the screen saver lock setting.	2008-12-16	10.0	CVE-2008-4237 CERT BID CONFIRM SECUNIA APPLE
aruba_networks -- aruba_mobility_controller aruba_networks -- aruba_mobility_controllers arubanetworks -- aruba_mobility_controller	Aruba Mobility Controller 2.4.8.x-FIPS, 2.5.x, 3.1.x, 3.2.x, 3.3.1.x, and 3.3.2.x allows remote attackers to cause a denial of service (device crash) via a malformed Extensible Authentication Protocol (EAP) frame.	2008-12-15	7.8	CVE-2008-5563 SECTRACK BID BUGTRAQ CONFIRM SECUNIA
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
aspapps -- asp_autodealer	SQL injection vulnerability in detail.asp in ASP AutoDealer allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2008-12-16	7.5	CVE-2008-5595 XF BID MILW0RM SECUNIA MISC
aspapps -- aspportal	Multiple SQL injection vulnerabilities in ASP Portal allow remote attackers to execute arbitrary SQL commands via the (1) ItemID parameter to classifieds.asp and the (2) ID parameter to Events.asp.	2008-12-16	7.5	CVE-2008-5605 XF BID MILW0RM
bpowerhouse -- mini_cms	Multiple directory traversal vulnerabilities in index.php in Mini CMS 1.0.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) page and (2) admin parameters.	2008-12-16	7.5	CVE-2008-5593 MILW0RM SECUNIA
bpowerhouse -- mini_blog	Multiple directory traversal vulnerabilities in index.php in Mini Blog 1.0.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) page and (2) admin parameters.	2008-12-16	7.5	CVE-2008-5594 MILW0RM SECUNIA
darkwet -- webcam_xp	Multiple array index errors in the HTTP server in Darkwet Network webcamXP 3.72.440.0 and earlier and beta 4.05.280 and earlier allow remote attackers to cause a denial of service (device crash) and read portions of memory via (1) an invalid camnum parameter to the pocketpc component and (2) an invalid id parameter to the show_gallery_pic component.	2008-12-18	9.4	CVE-2008-5674 BID BUGTRAQ SECUNIA
deltascripts -- php_shop	SQL injection vulnerability in admin/login.php in DeltaScripts PHP Shop 1.0 allows remote attackers to execute arbitrary SQL commands via the admin_username parameter. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5648 XF BID SECUNIA MILW0RM
digitalgreys -- com_contactinfo	SQL injection vulnerability in the Contact Information Module (com_contactinfo) component 1.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	2008-12-12	7.5	CVE-2008-5494 XF BID MILW0RM FRSIRT
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
dotnetindex -- professional_download_assistant	SQL injection vulnerability in admin/login.asp in Professional Download Assistant 0.1 allows remote attackers to execute arbitrary SQL commands via the (1) uname parameter (aka user field) or the (2) psw parameter (aka passwd field). NOTE: some of these details are obtained from third party information.	2008-12-15	7.5	CVE-2008-5571 BID MILW0RM SECUNIA OSVDB
gnu -- classpath	The gnu.java.security.util.PRNG class in GNU Classpath 0.97.2 and earlier uses a predictable seed based on the system time, which makes it easier for context-dependent attackers to conduct brute force attacks against cryptographic routines that use this class for randomness, as demonstrated against DSA private keys.	2008-12-17	7.5	CVE-2008-5659 MLIST CONFIRM
ibm -- websphere_portal	Unspecified vulnerability in IBM WebSphere Portal 6.0 before 6.0.1.5 has unknown impact and attack vectors related to "Access problems with BasicAuthTAI."	2008-12-18	10.0	CVE-2008-5675 CONFIRM
joomitaly -- jmovies	SQL injection vulnerability in the JMovies (aka JM or com_jmovies) component 1.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2008-12-16	7.5	CVE-2008-5607 BID MILW0RM
joomla -- com_books	SQL injection vulnerability in the Books (com_books) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the book_id parameter in a book_details action to index.php.	2008-12-17	7.5	CVE-2008-5643 XF BID MILW0RM
joomla -- joomla	PHP remote file inclusion vulnerability in index.php in Joomla! 1.0.11 through 1.0.14, when RG_EMULATION is enabled in configuration.php, allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter.	2008-12-18	7.5	CVE-2008-5671 CONFIRM
kalptaru_infotech -- product_sale_framework	SQL injection vulnerability in customer.forumtopic.php in Kalptaru Infotech Product Sale Framework 0.1 beta allows remote attackers to execute arbitrary SQL commands via the forum_topic_id parameter.	2008-12-16	7.5	CVE-2008-5590 BID MILW0RM
katywhitton -- rankem	SQL injection vulnerability in rankup.asp in Katy Whitton RankEm allows remote attackers to execute arbitrary SQL	2008-12-16	7.5	CVE-2008-5588 XF BID

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	commands via the siteID parameter.			MILW0RM
katywhitton -- rankem	SQL injection vulnerability in processlogin.asp in Katy Whitton RankEm allows remote attackers to execute arbitrary SQL commands via the (1) txtusername parameter (aka username field) or the (2) txtpassword parameter (aka password field). NOTE: some of these details are obtained from third party information.	2008-12-16	7.5	CVE-2008-5589 XF MILW0RM SECUNIA
kusaba -- kusaba	Multiple unrestricted file upload vulnerabilities in Kusaba 1.0.4 and earlier allow remote authenticated users to execute arbitrary code by uploading a file with an executable extension using (1) load_receiver.php or (2) a shipainter action to paint_save.php, then accessing the uploaded file via a direct request to this file in their user directory.	2008-12-18	9.0	CVE-2008-5663 XF XF BID BID MILW0RM MILW0RM
kwalbum -- kwalbum	Unrestricted file upload vulnerability in Kwalbum 2.0.4, 2.0.2, and earlier, when PICS_PATH is located in the web root, allows remote authenticated users with upload capability to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file under items/, related to the ReplaceBadFilenameChars function in include/ItemAdder.php. NOTE: some of these details are obtained from third party information.	2008-12-18	7.1	CVE-2008-5677 XF BID MILW0RM SECUNIA
lcxbbportal -- lcxbbportal	Multiple PHP remote file inclusion vulnerabilities in lcxBBportal 0.1 Alpha 2 allow remote attackers to execute arbitrary PHP code via a URL in the phpbb_root_path parameter to (1) portal/includes/portal_block.php and (2) includes/acp/acp_lcxbbportal.php.	2008-12-16	7.5	CVE-2008-5585 XF BID MILW0RM MISC
libvirt -- libvirt	Multiple methods in libvirt 0.3.2 through 0.5.1 do not check if a connection is read-only, which allows local users to bypass intended access restrictions and perform administrative actions.	2008-12-19	7.2	CVE-2008-5086 BID
merlix -- teamworx_server	SQL injection vulnerability in default.asp in Merlix Teamworx Server allows remote attackers to execute arbitrary SQL	2008-12-16	7.5	CVE-2008-5599 XF BID

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	commands via the password parameter (aka passwd field) in a login action. NOTE: some of these details are obtained from third party information.			MILW0RM SECUNIA
mini-pub -- mini-pub	mini-pub.php/front-end/cat.php in mini-pub 0.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the sFileName argument.	2008-12-15	7.5	CVE-2008-5580 BID BUGTRAQ
mini-pub -- mini-pub	PHP remote file inclusion vulnerability in mini-pub.php/front-end/img.php in mini-pub 0.3 allows remote attackers to execute arbitrary PHP code via a URL in the sFileName parameter.	2008-12-15	7.5	CVE-2008-5581 BID BUGTRAQ
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) and possibly trigger memory corruption via vectors related to (1) a reahable assertion or (2) an integer overflow.	2008-12-17	10.0	CVE-2008-5500 MISC MISC CONFIRM
mozilla -- firefox	Mozilla Firefox 2.x before 2.0.0.19 allows remote attackers to run arbitrary JavaScript with chrome privileges via vectors related to the feed preview, a different vulnerability than CVE-2008-3836.	2008-12-17	7.5	CVE-2008-5504 MISC CONFIRM
mplayer -- mplayer	Stack-based buffer overflow in the demux_open_vqf function in libmpdemux/demux_vqf.c in MPlayer 1.0 rc2 before r28150 allows remote attackers to execute arbitrary code via a malformed TwinVQ file.	2008-12-16	10.0	CVE-2008-5616 BID MISC CONFIRM CONFIRM SECUNIA
myiosoft -- easybookmarker	SQL injection vulnerability in plugins/bookmarker /bookmarker_backend.php in MyioSoft EasyBookMarker 4.0 allows remote attackers to execute arbitrary SQL commands via the Parent parameter.	2008-12-17	7.5	CVE-2008-5651 XF BID FRSIRT SECUNIA OSVDB MILW0RM
myiosoft -- easybookmarker	SQL injection vulnerability in the loginADP function in ajaxp.php in MyioSoft EasyBookMarker 4.0 allows remote attackers to execute arbitrary SQL commands via the rsargs parameter, as reachable through the username parameter.	2008-12-17	7.5	CVE-2008-5652 XF MILW0RM FRSIRT SECUNIA OSVDB

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	NOTE: some of these details are obtained from third party information.			
myiosoft -- easycalendar	SQL injection vulnerability in the loginADP function in ajaxp.php in MyioSoft EasyCalendar 4.0 allows remote attackers to execute arbitrary SQL commands via the rsargs parameter, as reachable through the username parameter, a different vector than CVE-2008-1344. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5654 XF SECUNIA OSVDB MILW0RM
myiosoft -- easybookmarker	Multiple SQL injection vulnerabilities in MyioSoft EasyBookMarker 4.0 allow remote attackers to execute arbitrary SQL commands via the (1) delete_folder and (2) delete_link parameters to unspecified vectors, possibly to (a) plugins/bookmarker/bookmarker_backend.php or (b) ajaxp.php, different vectors than CVE-2008-5654. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-12-17	7.5	CVE-2008-5655 FRSIRT
myiosoft.com -- ajaxportal	SQL injection vulnerability in the loginADP function in ajaxp.php in MyioSoft AjaxPortal 3.0 allows remote attackers to execute arbitrary SQL commands via the rsargs parameter, as reachable through the username parameter. NOTE: some of these details are obtained from third party information.	2008-12-17	7.5	CVE-2008-5653 SECUNIA OSVDB MILW0RM
netref -- netref	SQL injection vulnerability in Netref 4.0 allows remote attackers to execute arbitrary SQL commands via the id parameter to (1) fiche_product.php and (2) presentation.php.	2008-12-15	7.5	CVE-2008-5561 XF BID MILW0RM
nukedit -- nukedit	SQL injection vulnerability in utilities/login.asp in Nukedit 4.9.x, and possibly earlier, allows remote attackers to execute arbitrary SQL commands via the email parameter.	2008-12-15	7.5	CVE-2008-5582 BID MILW0RM
opera -- opera	The HTML parsing engine in Opera before 9.63 allows remote attackers to execute arbitrary code via crafted web pages that trigger an invalid pointer calculation and heap corruption.	2008-12-19	9.3	CVE-2008-5679 SECTRACK BUGTRAQ CONFIRM CONFIRM MISC
Back to top				

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
opera -- opera	Multiple buffer overflows in Opera before 9.63 might allow (1) remote attackers to execute arbitrary code via a crafted text area, or allow (2) user-assisted remote attackers to execute arbitrary code via a long host name in a file: URL.	2008-12-19	9.3	CVE-2008-5680 SECTRACK CONFIRM CONFIRM CONFIRM SECTRACK
opera -- opera	Unspecified vulnerability in Opera before 9.63 allows remote attackers to "reveal random data" via unknown vectors.	2008-12-19	7.8	CVE-2008-5683 CONFIRM CONFIRM SECTRACK
orb_networks -- orb	Directory traversal vulnerability in the media server in Orb Networks Orb before 2.01.0022 allows remote attackers to read arbitrary files via directory traversal sequences in an HTTP GET request.	2008-12-17	7.8	CVE-2008-5645 BID
parsblogger -- parsblogger	SQL injection vulnerability in blog.asp in ParsBlogger (Pb) allows remote attackers to execute arbitrary SQL commands via the wr parameter.	2008-12-17	7.5	CVE-2008-5637 BID MILW0RM FRSIRT
php -- php	PHP 5 before 5.2.7 does not properly initialize the page_uid and page_gid global variables for use by the SAPI php_getuid function, which allows context-dependent attackers to bypass safe_mode restrictions via variable settings that are intended to be restricted to root, as demonstrated by a setting of /etc for the error_log variable.	2008-12-17	7.5	CVE-2008-5624 XF BID BUGTRAQ CONFIRM SREASONRES
php -- php	PHP 5 before 5.2.7 does not enforce the error_log safe_mode restrictions when safe_mode is enabled through a php_admin_flag setting in httpd.conf, which allows context-dependent attackers to write to arbitrary files by placing a "php_value error_log" entry in a .htaccess file.	2008-12-17	7.5	CVE-2008-5625 XF BID CONFIRM SREASONRES
php -- php	Directory traversal vulnerability in the ZipArchive::extractTo function in PHP 5.2.6 and earlier allows context-dependent attackers to write arbitrary files via a ZIP file with a file whose name contains .. (dot dot) sequences.	2008-12-17	7.5	CVE-2008-5658 MISC CONFIRM MLIST
proclanmanager -- pro_clan_manager	Session fixation vulnerability in Pro Clan Manager 0.4.2 and earlier allows remote attackers to hijack web sessions by setting the PHPSESSID parameter.	2008-12-15	7.5	CVE-2008-5575 BID BUGTRAQ

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
quassel -- quassel_core	CRLF injection vulnerability in Quassel Core before 0.3.0.3 allows remote attackers to spoof IRC messages as other users via a crafted CTCP message.	2008-12-17	7.5	CVE-2008-5657 CONFIRM
realtek -- realtek_media_player	Stack-based buffer overflow in Realtek Media Player (aka Realtek Sound Manager, RtlRack, or rtlrack.exe) 1.15.0.0 allows remote attackers to execute arbitrary code via a crafted playlist (PLA) file.	2008-12-18	9.3	CVE-2008-5664 XF MISC BID MILW0RM SECUNIA OSVDB
roundcube -- roundcube_webmail	html2text.php in RoundCube Webmail (roundcubemail) 0.2-1.alpha and 0.2-3.beta allows remote attackers to execute arbitrary code via crafted input that is processed by the preg_replace function with the eval switch.	2008-12-16	10.0	CVE-2008-5619 FEDORA FEDORA MLIST MISC CONFIRM CONFIRM SECUNIA
roundcube -- roundcube_webmail	RoundCube Webmail (roundcubemail) before 0.2-beta allows remote attackers to cause a denial of service (memory consumption) via crafted size parameters that are used to create a large quota image.	2008-12-16	7.8	CVE-2008-5620 CONFIRM
rsyslog -- rsyslog	The ACL handling in rsyslog 3.12.1 to 3.20.0, 4.1.0, and 4.1.1 does not follow $AllowedSender directive, which allows remote attackers to bypass intended access restrictions and spoof log messages or create a large number of spurious messages.	2008-12-16	8.5	CVE-2008-5617 CONFIRM
scssboard -- scssboard	admin/forums.php in sCssBoard 1.0, 1.1, 1.11, and 1.12 allows remote attackers to bypass authentication and gain administrative access via a large value of the current_user[users_level] parameter.	2008-12-15	7.5	CVE-2008-5576 MILW0RM
scssboard -- scssboard	PHP remote file inclusion vulnerability in index.php in sCssBoard 1.0, 1.1, 1.11, and 1.12 allows remote attackers to execute arbitrary PHP code via a URL in the inc_function parameter.	2008-12-15	7.5	CVE-2008-5577 MILW0RM
scssboard -- scssboard	Multiple SQL injection vulnerabilities in index.php in sCssBoard 1.0, 1.1, 1.11, and 1.12 allow remote attackers to execute arbitrary SQL commands via (1) the f parameter in a showforum action, (2) the u	2008-12-15	7.5	CVE-2008-5578 BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	parameter in a profile action, (3) the viewcat parameter, or (4) a combination of scb_uid and scb_ident cookie values.			
sun -- java_wireless_toolkit_for_cldc	Multiple buffer overflows in Sun Java Wireless Toolkit (WTK) for CLDC 2.5.2 and earlier allow downloaded programs to execute arbitrary code via unknown vectors.	2008-12-17	9.3	CVE-2008-5662 SUNALERT SECUNIA
trac -- trac	Unspecified vulnerability in Trac before 0.11.2 allows attackers to cause a denial of service via unknown attack vectors related to "certain wiki markup."	2008-12-17	7.5	CVE-2008-5646 BID FRSIRT CONFIRM SECUNIA
turnkeyarcade -- turnkey_arcade_script	SQL injection vulnerability in index.php in Turnkey Arcade Script allows remote attackers to execute arbitrary SQL commands via the id parameter in a play action.	2008-12-17	7.5	CVE-2008-5629 BID SECUNIA MILW0RM
typo3 -- commerce_extension	SQL injection vulnerability in the Commerce extension 0.9.6 and earlier for TYPO3 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-12-16	7.5	CVE-2008-5609 FRSIRT CONFIRM CONFIRM
unscripts -- webmaster_marketplace	SQL injection vulnerability in member.php in Webmaster Marketplace allows remote attackers to execute arbitrary SQL commands via the u parameter.	2008-12-15	7.5	CVE-2008-5574 MILW0RM SECUNIA OSVDB
xoops -- xoops	SQL injection vulnerability in index.php in the xhresim module in XOOPS allows remote attackers to execute arbitrary SQL commands via the no parameter.	2008-12-18	7.5	CVE-2008-5665 XF BID MILW0RM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
apple -- mac_os_x apple -- mac_os_x_server	The kernel in Apple Mac OS X before 10.5.6 allows local users to cause a denial of service (infinite loop and system halt) by running an application that is dynamically linked to libraries on an NFS server, related to occurrence of an exception in this application.	2008-12-16	4.9	CVE-2008-4219 CERT BID CONFIRM SECUNIA APPLE
aspapps -- aspportal	ASPPortal stores sensitive information under the web root with insufficient access control, which allows remote attackers to download	2008-12-15	5.0	CVE-2008-5562 MILW0RM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	the database file via a direct request for xportal.mdb.			
aspapps -- aspticker	ASPTicker 1.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for news.mdb.	2008-12-16	5.0	CVE-2008-5603 XF MILW0RM SECUNIA
aspapps -- asp_autodealer	ASP AutoDealer stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for auto.mdb.	2008-12-16	5.0	CVE-2008-5608 XF MILW0RM MILW0RM
asterisk -- asterisk_business_edition asterisk -- open_source	Asterisk Open Source 1.2.26 through 1.2.30.3 and Business Edition B.2.3.5 through B.2.5.5, when realtime IAX2 users are enabled, allows remote attackers to cause a denial of service (crash) via authentication attempts involving (1) an unknown user or (2) a user using hostname matching.	2008-12-17	4.3	CVE-2008-5558 FRSIRT
avahi -- avahi	The originates_from_local_legacy_unicast_socket function (avahi-core/server.c) in avahi-daemon in Avahi before 0.6.24 allows remote attackers to cause a denial of service (crash) via a crafted mDNS packet with a source port of 0, which triggers an assertion failure.	2008-12-16	5.0	CVE-2008-5081 MLIST CONFIRM
barracuda_networks -- barracuda_spam_firewall	SQL injection vulnerability in index.cgi in the Account View page in Barracuda Spam Firewall (BSF) before 3.5.12.007 allows remote authenticated administrators to execute arbitrary SQL commands via a pattern_x parameter in a search_count_equals action, as demonstrated by the pattern_0 parameter.	2008-12-19	6.5	CVE-2008-1094 BUGTRAQ MILW0RM CONFIRM SECTRACK SECUNIA MISC
bonzacart -- bonza_cart	Cross-site request forgery (CSRF) vulnerability in admin/ad_settings.php in Bonza Cart 1.10 and earlier allows remote attackers to change the admin password via a logout action in conjunction with the NewAdmin, NewPass1, and NewPass2 parameters.	2008-12-15	6.8	CVE-2008-5567 MILW0RM SECUNIA
breach -- modsecurity	Multiple unspecified vulnerabilities in the ModSecurity (aka mod_security) module 2.5.0 through 2.5.5 for the Apache HTTP Server, when SecCacheTransformations is	2008-12-18	5.0	CVE-2008-5676 FRSIRT

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	enabled, allow remote attackers to cause a denial of service (daemon crash) or bypass the product's functionality via unknown vectors related to "transformation caching."			
check_up -- check_new	SQL injection vulnerability in findoffice.php in Check Up New Generation (aka Check New) 4.52, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the search parameter.	2008-12-16	6.8	CVE-2008-5586 BID MILW0RM SECUNIA
cmsmadesimple -- cms_made_simple	Directory traversal vulnerability in admin/login.php in CMS Made Simple 1.4.1 allows remote attackers to read arbitrary files via a .. (dot dot) in a cms_language cookie.	2008-12-17	5.0	CVE-2008-5642 BID MILW0RM FRSIRT SECUNIA
cold_bbs -- cold_bbs	Cold BBS stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for db/cforum.mdb.	2008-12-16	5.0	CVE-2008-5597 MILW0RM
dazzlindonna -- postecards	PostEcards stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for postcards.mdb.	2008-12-15	5.0	CVE-2008-5560 MILW0RM SECUNIA
dinkumsoft -- dl_paycart	Cross-site request forgery (CSRF) vulnerability in admin/settings.php in DL PayCart 1.34 and earlier allows remote attackers to change the admin password via a logout action in conjunction with the NewAdmin, NewPass1, and NewPass2 parameters.	2008-12-15	6.8	CVE-2008-5565 MILW0RM SECUNIA
dotnetindex -- professional_download_assistant	Professional Download Assistant 0.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for database/downloads.mdb.	2008-12-15	5.0	CVE-2008-5572 MILW0RM SECUNIA OSVDB
dotnetindex -- ikon_admanager	Ikon AdManager 2.1 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for ikonBAnner_AdManager.mdb.	2008-12-16	5.0	CVE-2008-5596 MILW0RM SECUNIA
Back to top				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
drennansoft -- my_simple_forum	Directory traversal vulnerability in index.php in My Simple Forum 3.0 and 4.1, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the action parameter.	2008-12-16	6.8	CVE-2008-5604 XF BID MILW0RM SECUNIA OSVDB
dxmsoft -- xm_easy_personal_ftp_server	XM Easy Personal FTP Server 5.6.0 allows remote authenticated users to cause a denial of service via a crafted argument to the NLST command, as demonstrated by a -1 argument.	2008-12-17	4.0	CVE-2008-5626 BID MILW0RM FRSIRT
fdgroup -- olib7_webview	Fretwell-Downing Informatics (FDI) OLIB7 WebView 2.5.1.1 allows remote authenticated users to obtain sensitive information from files via the infile parameter to the default URI under cgi/, as demonstrated by the (1) get_settings.ini, (2) setup.ini, and (3) text.ini files.	2008-12-18	4.0	CVE-2008-5678 XF BID MILW0RM
gazatem_technologies -- qmail_mailing_list_manager	Gazatem QMail Mailing List Manager 1.2 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for qmail.mdb.	2008-12-16	5.0	CVE-2008-5606 MILW0RM
gnome -- vinagre	Format string vulnerability in the vinagre_utils_show_error function (src/vinagre-utils.c) in Vinagre 0.5.x before 0.5.2 and 2.x before 2.24.2 might allow remote attackers to execute arbitrary code via a crafted URI or VNC server response.	2008-12-17	6.8	CVE-2008-5660 CONFIRM UBUNTU MANDRIVA FRSIRT MISC SECUNIA SECUNIA
gnu -- escript	Multiple buffer overflows in the (1) recognize_eps_file function (src/psgen.c) and (2) tilde_subst function (src/util.c) in GNU enscript 1.6.1, and possibly earlier, might allow remote attackers to execute arbitrary code via an epsf escape sequence with a long filename.	2008-12-19	6.8	CVE-2008-5078 CONFIRM SECTRACK REDHAT SECUNIA
ipn-mate -- ipn_pro_3	Cross-site request forgery (CSRF) vulnerability in admin/settings.php in IPN Pro 3 1.44 and earlier allows remote attackers to change the admin password via a logout action in conjunction with the admin_id, newpass_1, and newpass_2 parameters.	2008-12-15	6.8	CVE-2008-5568 MILW0RM SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
iwrite -- nightfall_personal_diary	Cross-site scripting (XSS) vulnerability in login.asp in Nightfall Personal Diary 1.0 allows remote attackers to inject arbitrary web script or HTML via the username parameter and possibly other "login fields." NOTE: some of these details are obtained from third party information.	2008-12-16	4.3	CVE-2008-5591 XF BID MILW0RM SECUNIA
iwrite -- nightfall_personal_diary	Nightfall Personal Diary 1.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for users-zza21.mdb.	2008-12-16	5.0	CVE-2008-5592 XF MILW0RM SECUNIA
joomla -- joomla	Joomla! 1.5.8 does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2008-12-19	5.0	CVE-2008-4122 BUGTRAQ BUGTRAQ MISC
little_cms -- little_cms	SQL injection vulnerability in index.php in CMS little 0.0.1 allows remote attackers to execute arbitrary SQL commands via the term parameter.	2008-12-17	6.8	CVE-2008-5628 BID MILW0RM
lovedesigner -- lito_lite_cms	SQL injection vulnerability in cate.php in Lito Lite CMS, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2008-12-17	6.8	CVE-2008-5636 MILW0RM FRSIRT SECUNIA
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in MediaWiki 1.13.0 through 1.13.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-12-19	4.3	CVE-2008-5249 MLIST
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in MediaWiki before 1.6.11, 1.12.x before 1.12.2, and 1.13.x before 1.13.3, when Internet Explorer is used and uploads are enabled, or an SVG scripting browser is used and SVG uploads are enabled, allows remote authenticated users to inject arbitrary web script or HTML by editing a wiki page.	2008-12-19	4.3	CVE-2008-5250 SECUNIA MLIST
mediawiki -- mediawiki	Cross-site request forgery (CSRF) vulnerability in the Special:Import feature in MediaWiki 1.3.0 through 1.6.10, 1.12.x before 1.12.2, and 1.13.x before 1.13.3 allows remote attackers to perform unspecified actions as authenticated users via unknown vectors.	2008-12-19	5.8	CVE-2008-5252 SECUNIA MLIST
Back to top				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
merlix -- teamworx_server	Merlix Teamworx Server stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for teamworx.mdb.	2008-12-16	5.0	CVE-2008-5600 XF MILW0RM SECUNIA
mini-pub -- mini-pub	Absolute path traversal vulnerability in mini-pub.php/front-end/cat.php in mini-pub 0.3 allows remote attackers to read arbitrary files via a full pathname in the sFileName parameter.	2008-12-15	5.0	CVE-2008-5579 BID BUGTRAQ
mozilla -- thunderbird	Mozilla Thunderbird 2.0.14 does not properly handle (1) multipart/mixed e-mail messages with many MIME parts and possibly (2) e-mail messages with many "Content-type: message/rfc822;" headers, which might allow remote attackers to cause a denial of service (stack consumption or other resource consumption) via a large e-mail message, a related issue to CVE-2006-1173.	2008-12-13	4.3	CVE-2008-5430 BUGTRAQ BUGTRAQ MISC
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 3.x before 3.0.5, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service via vectors that trigger an assertion failure.	2008-12-17	5.0	CVE-2008-5501 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 3.x before 3.0.5, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to cause a denial of service (crash) via vectors that trigger memory corruption, related to the GetXMLEntity and FastAppendChar functions.	2008-12-17	5.0	CVE-2008-5502 MISC CONFIRM
mozilla -- firefox	Mozilla Firefox 3.x before 3.0.5 allows remote attackers to bypass intended privacy restrictions by using the persist attribute in an XUL element to create and access data entities that are similar to cookies.	2008-12-17	5.0	CVE-2008-5505 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to bypass the same origin policy by causing the browser to issue an XMLHttpRequest to an attacker-	2008-12-17	6.8	CVE-2008-5506 MISC CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	controlled resource that uses a 302 redirect to a resource in a different domain, then reading content from the response, aka "response disclosure."			
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to bypass the same origin policy and access portions of data from another domain via a JavaScript URL that redirects to the target resource, which generates an error if the target data does not have JavaScript syntax, which can be accessed using the window.onerror DOM API.	2008-12-17	6.0	CVE-2008-5507 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 does not properly parse URLs with leading whitespace or control characters, which might allow remote attackers to misrepresent URLs and simplify phishing attacks.	2008-12-17	4.3	CVE-2008-5508 MISC MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The CSS parser in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 ignores the '\0' escaped null character, which might allow remote attackers to bypass protection mechanisms such as sanitization routines.	2008-12-17	5.0	CVE-2008-5510 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allows remote attackers to bypass the same origin policy and conduct cross-site scripting (XSS) attacks via an XBL binding to an "unloaded document."	2008-12-17	4.3	CVE-2008-5511 MISC MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 allow remote attackers to run arbitrary JavaScript with chrome privileges via unknown vectors in which "page content can pollute XPCNativeWrappers."	2008-12-17	6.8	CVE-2008-5512 MISC MISC CONFIRM
Back to top				

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
mozilla -- firefox	Unspecified vulnerability in the session-restore feature in Mozilla Firefox 3.x before 3.0.5 and 2.x before 2.0.0.19 allows remote attackers to bypass the same origin policy, inject content into documents associated with other domains, and conduct cross-site scripting (XSS) attacks via unknown vectors related to restoration of SessionStore data.	2008-12-17	4.3	CVE-2008-5513 CONFIRM
natterchat -- natterchat	Natterchat 1.12 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for natterchat112.mdb.	2008-12-16	5.0	CVE-2008-5602 XF MILW0RM
opera -- opera	Opera before 9.63 does not block unspecified "scripted URLs" during the feed preview, which allows remote attackers to read existing subscriptions and force subscriptions to arbitrary feed URLs.	2008-12-19	4.3	CVE-2008-5681 SECTRACK CONFIRM CONFIRM
opera -- opera	Cross-site scripting (XSS) vulnerability in Opera before 9.63 allows remote attackers to inject arbitrary web script or HTML via built-in XSLT templates.	2008-12-19	4.3	CVE-2008-5682 SECTRACK CONFIRM CONFIRM
orb_networks -- orb	Unspecified vulnerability in the media server in Orb Networks Orb before 2.01.0025 allows remote attackers to cause a denial of service (daemon crash) via a malformed HTTP request.	2008-12-15	5.0	CVE-2008-5564 BID BUGTRAQ SECUNIA
php_multiple_newsletters -- php_multiple_newsletters	Directory traversal vulnerability in index.php in PHP Multiple Newsletters 2.7, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	2008-12-15	6.8	CVE-2008-5570 BID MILW0RM SECUNIA
phparanoid -- phparanoid	Multiple cross-site request forgery (CSRF) vulnerabilities in PHParanoid before 0.4 allow remote attackers to perform unspecified actions as authenticated users via (1) unknown vectors involving admin.php and (2) unknown vectors related to private messages.	2008-12-18	6.8	CVE-2008-5672 XF CONFIRM SECUNIA
phparanoid -- phparanoid	PHParanoid before 0.4 does not properly restrict access to the members area by unauthenticated users, which has unknown impact and remote attack vectors.	2008-12-18	6.5	CVE-2008-5673 CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
phppeppershop -- phppeppershop	Multiple cross-site scripting (XSS) vulnerabilities in PHPepperShop 1.4 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) index.php or (2) shop/kontakt.php, or (3) shop_kunden_mgmt.php or (4) SHOP_KONFIGURATION.php in shop/Admin/.	2008-12-15	4.3	CVE-2008-5569 XF BID BUGTRAQ SECUNIA OSVDB OSVDB OSVDB OSVDB
phpmultiplenewsletters -- phpmultiplenewsletters	Cross-site scripting (XSS) vulnerability in index.php in Triangle Solutions PHP Multiple Newsletters 2.7 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2008-12-15	4.3	CVE-2008-5566 BID MILW0RM SECUNIA
phpmyadmin -- phpmyadmin	Cross-site request forgery (CSRF) vulnerability in phpMyAdmin 2.11.x before 2.11.9.4 and 3.x before 3.1.1.0 allows remote attackers to perform unauthorized actions as the administrator via a link or IMG tag to tbl_structure.php with a modified table parameter. NOTE: this can be leveraged to conduct SQL injection attacks and execute arbitrary code.	2008-12-16	6.0	CVE-2008-5621 BID CONFIRM
phpmyadmin -- phpmyadmin	Multiple cross-site request forgery (CSRF) vulnerabilities in phpMyAdmin 2.11.x before 2.11.9.4 and 3.x before 3.1.1.0 allow remote attackers to conduct SQL injection attacks via unknown vectors related to the table parameter, a different vector than CVE-2008-5621.	2008-12-16	6.0	CVE-2008-5622 FEDORA FEDORA CONFIRM SECUNIA
phpmygallery -- phpmygallery	Directory traversal vulnerability in index.php in PHPmyGallery 1.51 gold allows remote attackers to list arbitrary directories via a .. (dot dot) in the group parameter.	2008-12-16	5.0	CVE-2008-5598 BID MILW0RM
phppgadmin -- phppgadmin	Directory traversal vulnerability in libraries/lib.inc.php in phpPgAdmin 4.2.1 and earlier, when register_globals is enabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the _language parameter to index.php.	2008-12-16	4.3	CVE-2008-5587 BID MILW0RM SECUNIA
projectpier -- projectpier	Cross-site request forgery (CSRF) vulnerability in index.php in ProjectPier 0.8 and earlier allows remote attackers to perform actions as an administrator via the query string, as demonstrated by a delete	2008-12-15	6.8	CVE-2008-5583 BID CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	project action.			
projectpier -- projectpier	Multiple cross-site scripting (XSS) vulnerabilities in ProjectPier 0.8 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) a message, (2) a milestone, or (3) a display name in a profile, or the (4) a or (5) c parameter to index.php.	2008-12-15	4.3	CVE-2008-5584 CONFIRM
qualityunit -- post_affiliate_pro	SQL injection vulnerability in merchants/index.php in Post Affiliate Pro 3 and 3.1.4 allows remote attackers to execute arbitrary SQL commands via the umprof_status parameter.	2008-12-17	6.8	CVE-2008-5630 XF BID MILW0RM FRSIRT SECUNIA
robs-projects -- asp_user_engine	User Engine Lite ASP stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for users.mdb.	2008-12-16	5.0	CVE-2008-5601 MILW0RM SECUNIA OSVDB
rsyslog -- rsyslog	imudp in rsyslog 4.x before 4.1.2, 3.21 before 3.21.9 beta, and 3.20 before 3.20.2 generates a message even when it is sent by an unauthorized sender, which allows remote attackers to cause a denial of service (disk consumption) via a large number of spurious messages.	2008-12-16	5.0	CVE-2008-5618 CONFIRM
sun -- opensolaris sun -- solaris	The IPv4 Forwarding feature in Sun Solaris 10 and OpenSolaris snv_47 through snv_82, with certain patches installed, allows remote attackers to cause a denial of service (panic) via unknown vectors that trigger a NULL pointer dereference.	2008-12-17	5.4	CVE-2008-5661 SUNALERT
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the X Inter Client Exchange library (aka libICE) in Sun Solaris 8 through 10 and OpenSolaris before snv_85 allows context-dependent attackers to cause a denial of service (application crash), as demonstrated by a port scan that triggers a segmentation violation in the Gnome session manager (aka gnome-session).	2008-12-19	5.0	CVE-2008-5684 SUNALERT CONFIRM
textpattern -- textpattern	Multiple cross-site scripting (XSS) vulnerabilities in Textpattern (aka Txp CMS) 4.0.5 allow remote attackers to inject arbitrary web script or HTML via (1) the PATH_INFO to setup/index.php or (2) the name parameter to index.php in the	2008-12-18	4.3	CVE-2008-5668 BID CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	comments preview section.			
textpattern -- textpattern	index.php in the comments preview section in Textpattern (aka Txp CMS) 4.0.5 allows remote attackers to cause a denial of service via a long message parameter.	2008-12-18	5.0	CVE-2008-5669 BID CONFIRM
textpattern -- textpattern	Textpattern (aka Txp CMS) 4.0.5 does not ask for the old password during a password reset, which makes it easier for remote attackers to change a password after hijacking a session.	2008-12-18	6.8	CVE-2008-5670 BID BUGTRAQ SECUNIA
trac -- trac	Unspecified vulnerability in the HTML sanitizer filter in Trac before 0.11.2 allows attackers to conduct phishing attacks via unknown attack vectors.	2008-12-17	5.0	CVE-2008-5647 BID FRSIRT CONFIRM SECUNIA
txtblogcms -- txtblog	Directory traversal vulnerability in index.php in TxtBlog 1.0 Alpha allows remote attackers to read arbitrary files via a .. (dot dot) in the m parameter.	2008-12-17	4.3	CVE-2008-5639 XF BID MILW0RM
typo3 -- typo3	Cross-site scripting (XSS) vulnerability in the frontend plugin for the felogin system extension in TYPO3 4.2.0, 4.2.1 and 4.2.2 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2008-12-17	4.3	CVE-2008-5656 CONFIRM
typosphere -- typo	Cross-site scripting (XSS) vulnerability in the file backend module in TYPO3 4.2.2 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2008-12-17	4.3	CVE-2008-5644 FRSIRT CONFIRM SECUNIA
virusblokada -- vba32_personal_antivirus	The scanning engine in VirusBlokAda VBA32 Personal Antivirus 3.12.8.x allows remote attackers to cause a denial of service (memory corruption and application crash) via a malformed RAR archive.	2008-12-18	5.0	CVE-2008-5667 BID MILW0RM

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
barracuda_networks -- barracuda_im_firewall barracuda_networks -- barracuda_load_balancer barracuda_networks -- barracuda_message_archiver	Multiple cross-site scripting (XSS) vulnerabilities in index.cgi in Barracuda Spam Firewall (BSF) before 3.5.12.007, Message Archiver before 1.2.1.002, Web Filter before 3.3.0.052, IM Firewall before 3.1.01.017, and Load Balancer before 2.3.024 allow remote	2008-12-19	3.5	CVE-2008-0971 BUGTRAQ OSVDB CONFIRM SECTRACK SECUNIA

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
barracuda_networks -- barracuda_spam_firewall barracuda_networks -- barracuda_web_filter	attackers to inject arbitrary web script or HTML via (1) the Policy Name field in Search Based Retention Policy in Message Archiver; unspecified parameters in the (2) IP Configuration, (3) Administration, (4) Journal Accounts, (5) Retention Policy, and (6) GroupWise Sync components in Message Archiver; (7) input to search operations in Web Filter; and (8) input used in error messages and (9) hidden INPUT elements in (a) Spam Firewall, (b) IM Firewall, and (c) Web Filter.			MISC
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The loadBindingDocument function in Mozilla Firefox 2.x before 2.0.0.19, Thunderbird 2.x before 2.0.0.19, and SeaMonkey 1.x before 1.1.14 does not perform any security checks related to the same-domain policy, which allows remote attackers to read or access data from other domains via crafted XBL bindings.	2008-12-17	2.6	CVE-2008-5503 MISC CONFIRM
wftpserver -- winftp_ftp_server	WinFTP FTP Server 2.3.0, when passive (aka PASV) mode is used, allows remote authenticated users to cause a denial of service via a sequence of FTP sessions that include an invalid "NLST -1" command.	2008-12-18	3.5	CVE-2008-5666 MILW0RM FRSIRT SECUNIA
Back to top				