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

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

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

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

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score
SUSE Linux -- Emacs	Emacs in SUSE Linux imports Python script from the current working directory during editing of a Python file, which allows local users to execute arbitrary code via a Trojan horse Python file.	2008-09-22	7.2
E-Php CMS	SQL injection vulnerability in article.php in E-Php CMS allows remote attackers to execute arbitrary SQL commands via the es_id parameter.	2008-09-24	7.5
RazorCommerce -- Shopping Cart	SQL injection vulnerability in category_search.php in RazorCommerce Shopping Cart allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-09-24	7.5
ACG-ScriptShop --E-Gold Script Shop	SQL injection vulnerability in index.php in ACG-ScriptShop E-Gold Script Shop allows remote attackers to execute arbitrary SQL commands via the cid parameter in a showcat action.	2008-09-24	7.5
Diesel Joke Site	SQL injection vulnerability in picture_category.php in Diesel Joke Site allows remote attackers to execute arbitrary SQL commands via the id parameter, a different	2008-09-24	7.5

	vector than CVE-2006-3763.			
Cars & Vehicles	SQL injection vulnerability in page.php in Cars & Vehicle (aka Cars-Vehicle Script) allows remote attackers to execute arbitrary SQL commands via the lnkid parameter.	2008-09-22	7.5	C
Pre Real Estate Listings	SQL injection vulnerability in search.php in Pre Real Estate Listings allows remote attackers to execute arbitrary SQL commands via the c parameter.	2008-09-23	7.5	C
CMS Portal Edition	SQL injection vulnerability in index.php in webCMS Portal Edition allows remote attackers to execute arbitrary SQL commands via the id parameter in a documentos action, a different vector than CVE-2008-3213.	2008-09-23	7.5	C
CMS Portal Edition	SQL injection vulnerability in index.php in webCMS Portal Edition allows remote attackers to execute arbitrary SQL commands via the id_doc parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-23	7.5	C
SoftAcid hotel Reservation System (HRS)	SQL injection vulnerability in city.asp in SoftAcid Hotel Reservation System (HRS) allows remote attackers to execute arbitrary SQL commands via the city parameter.	2008-09-24	7.5	C
alt-n -- securitygateway	Stack-based buffer overflow in SecurityGateway.dll in Alt-N Technologies SecurityGateway 1.0.1 allows remote attackers to execute arbitrary code via a long username parameter.	2008-09-24	10.0	C
asp_indir -- fot_video_scripti	SQL injection vulnerability in izle.asp in FoT Video scripti 1.1 beta allows remote attackers to execute arbitrary SQL commands via the oyun parameter.	2008-09-23	7.5	C
attachmax -- dolphin	SQL injection vulnerability in index.php in Attachmax Dolphin 2.1.0 and earlier allows remote attackers to execute arbitrary SQL commands via the category parameter in a Search action.	2008-09-24	7.5	C
attachmax -- dolphin	PHP remote file inclusion vulnerability in config.php in Attachmax Dolphin 2.1.0 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the rel_path parameter.	2008-09-24	7.5	C
audiocoding -- faad2	Heap-based buffer overflow in the decodeMP4file function (frontend/main.c) in FAAD2 before 2.6.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted MPEG-4 (MP4) file.	2008-09-24	9.3	C
cj -- ultra_plus	SQL injection vulnerability in CJ Ultra Plus 1.0.4 and earlier allows remote attackers to execute arbitrary SQL	2008-09-25	7.5	C

	commands via an SID cookie.		
czaries -- czarnews	SQL injection vulnerability in cn_users.php in CzarNews 1.20 and earlier allows remote attackers to execute arbitrary SQL commands via a recook cookie.	2008-09-24	7.5
downline_goldmine -- builder downline_goldmine -- new_addon	SQL injection vulnerability in tr.php in DownlineGoldmine Special Category Addon, Downline Builder Pro, New Addon, and Downline Goldmine Builder allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: some of these details are obtained from third party information.	2008-09-23	7.5
drupal -- mailhandler	SQL injection vulnerability in the Mailhandler module 5.x before 5.x-1.4 and 6.x before 6.x-1.4, a module for Drupal, allows remote attackers to execute arbitrary SQL commands via unspecified vectors, related to composing queries without using the Drupal database API.	2008-09-24	7.5
epic_games -- unreal_tournament_3	Directory traversal vulnerability in ImageServer (aka UTImageServer) in WebAdmin before 1.7 for Epic Games Unreal Tournament 3 (UT3) 1.3 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	2008-09-25	7.8
freebsd -- freebsd netbsd -- netbsd openbsd -- openbsd	ftpd in OpenBSD 4.3, FreeBSD 7.0, and NetBSD 4.0 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.	2008-09-25	7.5
gonafish -- linkscaffepro	SQL injection vulnerability in index.php in Gonafish LinksCaffePRO 4.5 allows remote attackers to execute arbitrary SQL commands via the idd parameter in a deadlink action.	2008-09-24	7.5
invision_power_services -- invision_power_board	SQL injection vulnerability in xmlout.php in Invision Power Board (IP.Board or IPB) 2.2.x and 2.3.x allows remote attackers to execute arbitrary SQL commands via the name parameter.	2008-09-22	7.5
isc -- bind	Unspecified vulnerability in ISC BIND 9.3.5-P2-W1, 9.4.2-P2-W1, and 9.5.0-P2-W1 on Windows allows remote attackers to cause a denial of service (UDP client handler termination) via unknown vectors.	2008-09-22	7.8
mozilla -- firefox mozilla -- seamonkey	Stack-based buffer overflow in the URL parsing implementation in Mozilla Firefox before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to execute arbitrary code via a crafted UTF-8 URL in a link.	2008-09-24	10.0

mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The nsXMLDocument::OnChannelRedirect function in Mozilla Firefox before 2.0.0.17, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass the Same Origin Policy and execute arbitrary JavaScript code via unknown vectors.	2008-09-24	7.5
mozilla -- firefox	feedWriter in Mozilla Firefox before 2.0.0.17 allows remote attackers to execute scripts with chrome privileges via vectors related to feed preview and the (1) elem.doCommand, (2) elem.dispatchEvent, (3) _setTitleText, (4) _setTitleImage, and (5) _initSubscriptionUI functions.	2008-09-24	7.5
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, and SeaMonkey before 1.1.12, allow user-assisted remote attackers to move a window during a mouse click, and possibly force a file download or unspecified other drag-and-drop action, via a crafted onmousedown action that calls window.moveBy, a variant of CVE-2003-0823.	2008-09-24	9.3
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The XPConnect component in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to "pollute XPCNativeWrappers" and execute arbitrary code with chrome privileges via vectors related to (1) chrome XBL and (2) chrome JS.	2008-09-24	7.5
mozilla -- firefox	The XPConnect component in Mozilla Firefox before 2.0.0.17 allows remote attackers to "pollute XPCNativeWrappers" and execute arbitrary code with chrome privileges via vectors related to a SCRIPT element.	2008-09-24	7.5
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to create documents that lack script-handling objects, and execute arbitrary code with chrome privileges, via vectors related to (1) the document.loadBindingDocument function and (2) XSLT.	2008-09-24	7.5
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Integer overflow in the MathML component in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via an mtd element with a large integer value in the rowspan attribute, related to the layout engine.	2008-09-24	10.0
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Multiple unspecified vulnerabilities in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the JavaScript engine and (1) misinterpretation of the characteristics of Namespace and QName in jsxml.c, (2) misuse of signed integers in the	2008-09-24	10.0

	nsEscapeCount function in nsEscape.cpp, and (3) interaction of JavaScript garbage collection with certain use of an NPObject in the nsNPObjWrapper::GetNewOrUsed function in nsJSNPRuntime.cpp.		
mozilla -- firefox	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to the layout engine and (1) a zero value of the "this" variable in the nsContentList::Item function; (2) interaction of the indic IME extension, a Hindi language selection, and the "g" character; and (3) interaction of the nsFrameList::SortByContentOrder function with a certain insufficient protection of inline frames.	2008-09-24	10.0
mozilla -- firefox	Multiple unspecified vulnerabilities in Mozilla Firefox 3.x before 3.0.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to graphics rendering and (1) handling of a long alert messagebox in the cairo_surface_set_device_offset function, (2) integer overflows when handling animated PNG data in the info_callback function in nsPNGDecoder.cpp, and (3) an integer overflow when handling SVG data in the nsSVGFEGaussianBlurElement::SetupPredivide function in nsSVGFilters.cpp.	2008-09-24	10.0
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allows remote attackers to bypass "restrictions imposed on local HTML files," and obtain sensitive information and prompt users to write this information into a file, via directory traversal sequences in a resource: URI.	2008-09-24	7.8
osads_alliance_database -- osads_alliance_database	Unspecified vulnerability in OSADS Alliance Database before 2.1 has unknown impact and attack vectors, possibly related to includes/functions.php, a different issue than CVE-2006-2874.	2008-09-24	10.0
php_crawler -- php_crawler	PHP remote file inclusion vulnerability in footer.php in PHP-Crawler 0.8 allows remote attackers to execute arbitrary PHP code via a URL in the footer_file parameter.	2008-09-24	7.5
proarcadescript -- proarcadescript	SQL injection vulnerability in ProArcadeScript 1.3 allows remote attackers to execute arbitrary SQL commands via the random parameter to the default URI.	2008-09-22	7.5
rianxosencabos_cms -- rianxosencabos_cms	Rianxosencabos CMS 0.9 allows remote attackers to bypass authentication and gain administrative access by setting the usuario and pass cookies to 1.	2008-09-25	7.5

technote -- technote	PHP remote file inclusion vulnerability in skin_shop/standard/3_plugin_twindow/twindow_notice.php in Technote 7 allows remote attackers to execute arbitrary PHP code via a URL in the shop_this_skin_path parameter.	2008-09-24	10.0	C
typo3 -- secure_directory	Unspecified vulnerability in the TYPO3 Secure Directory (kw_secdir) extension before 1.0.2 allows remote attackers to execute arbitrary code via unknown vectors related to "injection of control characters."	2008-09-23	10.0	C
x10media -- .x10_automatic_mp3_script	Multiple PHP remote file inclusion vulnerabilities in x10Media x10 Automatic MP3 Script 1.5.5 allow remote attackers to execute arbitrary PHP code via a URL in the web_root parameter to (1) includes/function_core.php and (2) templates/layout_lyrics.php.	2008-09-24	7.5	C
xerox -- workcentre xerox -- workcentre_pro	Buffer overflow in the printer sharing services in the Samba code in Xerox ESS/Network Controller in Pro 2xx Series before *.60.22.016, 7655/7665/7675 products before 040.033.53050, and 56xx Series before 21.113.02.015 allows remote attackers to modify system configuration via unknown attack vectors related to "Remote Service Message Block (SMB) responses." NOTE: due to insufficient details, it is unclear whether this is a duplicate of an existing CVE identifier for Samba.	2008-09-23	10.0	C

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Mantis	Mantis does not set the secure flag for the session cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.	2008-09-24	5.0	CVE-2008-3102 BUGTRAQ MISC
Drupal 5.10, 6.4	Drupal, probably 5.10 and 6.4, does not set the secure flag for the session cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.	2008-09-23	5.0	CVE-2008-3661 BID MISC
CMS Portal Edition	Cross-site scripting (XSS) vulnerability in index.php in webCMS Portal Edition allows	2008-09-23	4.3	CVE-2008-4184 BID SECUNIA

	remote attackers to inject arbitrary web script or HTML via the patron parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.			
ProActive CMS	Directory traversal vulnerability in index.php in ProActive CMS allows remote attackers to read arbitrary files via a .. (dot dot) in the template parameter.	2008-09-23	4.3	CVE-2008-4187 XF MILW0RM
addalink -- addalink	SQL injection vulnerability in user_read_links.php in Addalink 1.0 beta 4 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the category_id parameter.	2008-09-24	6.8	CVE-2008-4145 MILW0RM FRSIRT
addalink -- addalink	Addalink 1.0 beta 4 and earlier allows remote attackers to (1) approve web-site additions via a modified approved field and (2) change the visit-counter value via a modified counter field.	2008-09-24	5.0	CVE-2008-4146 MILW0RM FRSIRT
assetman -- assetman	SQL injection vulnerability in search_inv.php in Assetman 2.5b allows remote attackers to execute arbitrary SQL commands and conduct session fixation attacks via a combination of crafted order and order_by parameters in a search_all action.	2008-09-22	6.8	CVE-2008-4161 BID MILW0RM SECUNIA
attachmax -- dolphin	Attachmax Dolphin 2.1.0 and earlier does not properly protect info.php in the main folder, which allows remote attackers to obtain sensitive information via a direct request.	2008-09-24	5.0	CVE-2008-4207 BID BUGTRAQ MILW0RM MISC
benjamin_kuz -- dynamic_mp3_lister	Multiple cross-site scripting (XSS) vulnerabilities in index.php in Dynamic MP3 Lister 2.0.1 allow remote attackers to inject arbitrary web script or HTML via the (1) currentpath, (2) invert, (3)	2008-09-23	4.3	CVE-2008-4174 XF BID MISC

	search, and (4) sort parameters.			
cyask -- cyask	Directory traversal vulnerability in collect.php in CYASK 3.x allows remote attackers to read arbitrary files via a .. (dot dot) in the neturl parameter.	2008-09-24	5.0	CVE-2008-4151 BUGTRAQ MILW0RM
denora_irc_stats -- denora_irc_stats	Unspecified vulnerability in Denora IRC Stats Server before 1.4.1 allows remote IRC servers to cause a denial of service (application crash) via a crafted CTCP response.	2008-09-25	5.0	CVE-2008-4246 CONFIRM
drupal -- mailsave	Cross-site scripting (XSS) vulnerability in the Mailsave module 5.x before 5.x-3.3 and 6.x before 6.x-1.3, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via an e-mail message with an attached file that has a modified Content-Type.	2008-09-24	4.3	CVE-2008-4147 CONFIRM
drupal -- link_to_us	Cross-site scripting (XSS) vulnerability in the Greg Holsclaw Link to Us module 5.x before 5.x-1.1 for Drupal allows remote authenticated users to inject arbitrary web script or HTML via the "Link page header" field.	2008-09-24	4.3	CVE-2008-4149 CONFIRM
drupal -- talk	The Talk module 5.x before 5.x-1.3 and 6.x before 6.x-1.5, a module for Drupal, does not perform access checks for a node before displaying comments, which allows remote attackers to obtain sensitive information.	2008-09-24	5.0	CVE-2008-4153 CONFIRM
emacspeak_inc -- emacspeak	extract-table.pl in Emacspeak 26 and 28 allows local users to overwrite arbitrary files via a symlink attack on the extract-table.csv temporary file.	2008-09-24	6.6	CVE-2008-4191 CONFIRM XF BID SECUNIA CONFIRM
fuzzylime -- fuzzylime_cms	Cross-site scripting (XSS) vulnerability in admin/usercheck.php in fuzzylime (cms) before 3.03 allows remote attackers to inject	2008-09-24	4.3	CVE-2008-3098 FRSIRT SECUNIA CONFIRM

	arbitrary web script or HTML via the user parameter to the login form.			
horde -- turba_contact_manager_h3	Cross-site scripting (XSS) vulnerability in imp/test.php in Horde Turba Contact Manager H3 2.2.1, and possibly other Horde Project products, allows remote attackers to inject arbitrary web script or HTML via the User field in an IMAP session.	2008-09-23	4.3	CVE-2008-4182 XF BID MISC
integramod -- integramod	IntegraMOD 1.4.x stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a backup via a direct request to a backup/backup-yyyy-dd-mm.sql filename.	2008-09-23	5.0	CVE-2008-4183 BID MILW0RM CONFIRM SECUNIA
linkbidscript -- linkbidscript	Multiple SQL injection vulnerabilities in Link Bid Script 1.5 allow remote attackers to execute arbitrary SQL commands via the (1) ucat parameter to upgrade.php and the (2) id parameter to linkadmin/edit.php.	2008-09-23	6.5	CVE-2008-4175 BID MILW0RM
michael_roth_software -- pftp	Michael Roth Software Personal FTP Server (PFT) 6.0f allows remote attackers to cause a denial of service (service crash) via multiple RETR commands, possibly involving long filenames.	2008-09-24	5.0	CVE-2008-4136 BID MILW0RM MISC SECUNIA
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 allow remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via byte order mark (BOM) characters that are removed from JavaScript code before execution, aka "Stripped BOM characters bug."	2008-09-24	4.3	CVE-2008-4065 CONFIRM CONFIRM

mozilla -- firefox	Mozilla Firefox 2.0.0.14, and other versions before 2.0.0.17, allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via HTML-escaped low surrogate characters that are ignored by the HTML parser, as demonstrated by a "jav?ascript" sequence, aka "HTML escaped low surrogates bug."	2008-09-24	4.3	CVE-2008-4066 CONFIRM MISC CONFIRM MISC
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Directory traversal vulnerability in Mozilla Firefox before 2.0.0.17 and 3.x before 3.0.2, Thunderbird before 2.0.0.17, and SeaMonkey before 1.1.12 on Linux allows remote attackers to read arbitrary files via a .. (dot dot) and URL-encoded / (slash) characters in a resource: URI.	2008-09-24	4.3	CVE-2008-4067 CONFIRM CONFIRM CONFIRM MISC
mozilla -- firefox mozilla -- seamonkey	The XBM decoder in Mozilla Firefox before 2.0.0.17 and SeaMonkey before 1.1.12 allows remote attackers to read uninitialized memory, and possibly obtain sensitive information in opportunistic circumstances, via a crafted XBM image file.	2008-09-24	5.0	CVE-2008-4069 CONFIRM CONFIRM MISC
netenberg -- fantastico_de_luxe	Directory traversal vulnerability in includes/xml.php in the Netenberg Fantastico De Luxe module before 2.10.4 r19 for cPanel, when cPanel PHP Register Globals is enabled, allows remote authenticated users to include and execute arbitrary local files via a .. (dot dot) or absolute pathname in the fantasticopath parameter. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2.sftp URL.	2008-09-23	6.8	CVE-2008-4181 BID CONFIRM
nooms -- nooms	Open redirect vulnerability in admin/auth.php in NooMS 1.1	2008-09-22	4.3	CVE-2008-4162 BUGTRAQ

	allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the g_site_url parameter.			
nooms -- nooms	Multiple cross-site scripting (XSS) vulnerabilities in NooMS 1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) page_id parameter to smileys.php and the (2) q parameter to search.php.	2008-09-23	4.3	CVE-2008-4179 XF BID BUGTRAQ SECUNIA
nooms -- nooms	Unspecified vulnerability in db.php in NooMS 1.1 allows remote attackers to conduct brute force attacks against passwords via a username in the g_dbuser parameter and a password in the g_dbpwd parameter, and possibly a "localhost" g_dbhost parameter value, related to a "Mysql Remote Brute Force Vulnerability."	2008-09-23	5.0	CVE-2008-4180 XF BUGTRAQ
opensolution -- quick.cart	Cross-site scripting (XSS) vulnerability in admin.php in Quick.Cart 3.1 allows remote attackers to inject arbitrary web script or HTML via the query string.	2008-09-24	4.3	CVE-2008-4140 BID BUGTRAQ
openswan -- openswan	The IPSEC livetest tool in Openswan 2.4.4 and earlier allows local users to overwrite arbitrary files and execute arbitrary code via a symlink attack on the (1) ipseclive.conn and (2) ipsec.olts.remote.log temporary files.	2008-09-24	4.4	CVE-2008-4190 CONFIRM XF BID CONFIRM
oscommerce -- oscommerce	create_account.php in osCommerce 2.2 RC 2a allows remote attackers to obtain sensitive information via an invalid dob parameter, which reveals the installation path in an error message.	2008-09-22	5.0	CVE-2008-4170 XF BID BUGTRAQ
pdnsd -- pdnsd	The p_exec_query function in src/dns_query.c in pdnsd before	2008-09-24	5.0	CVE-2008-4194 CONFIRM

	1.2.7-par allows remote attackers to cause a denial of service (daemon crash) via a long DNS reply with many entries in the answer section, related to a "dangling pointer bug."			CONFIRM FRSIRT
proftpd_project -- proftpd	ProFTPD 1.3.1 interprets long commands from an FTP client as multiple commands, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks and execute arbitrary FTP commands via a long ftp:// URI that leverages an existing session from the FTP client implementation in a web browser.	2008-09-25	6.8	CVE-2008-4242 XF BID SECUNIA CONFIRM
redhat -- jboss_enterprise_application_platform	The default configuration of the JBossAs component in Red Hat JBoss Enterprise Application Platform (aka JBossEAP or EAP), possibly 4.2 before CP04 and 4.3 before CP02, when a production environment is enabled, sets the DownloadServerClasses property to true, which allows remote attackers to obtain sensitive information (non-EJB classes) via a download request, a different vulnerability than CVE-2008-3273.	2008-09-23	4.3	CVE-2008-3519 MISC MISC
rianxosencabos_cms -- rianxosencabos_cms	The Admin Control Panel in Rianxosencabos CMS 0.9 does not require administrator privileges, which allows remote authenticated users to (1) change a user's privileges, (2) delete a user account, or perform unspecified other administrative actions via vectors involving an admin lista action to the default URI, possibly related to useradmin.php.	2008-09-25	6.5	CVE-2008-4245 XF BID MILW0RM
squirrelmail -- squirrelmail	Squirrelmail 1.4.15 does not set the secure flag for the session	2008-09-24	5.0	CVE-2008-3663 BID

	cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.			BUGTRAQ MISC
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the UFS module in Sun Solaris 8 through 10 and OpenSolaris allows local users to cause a denial of service (NULL pointer dereference and kernel panic) via unknown vectors related to the Solaris Access Control List (ACL) implementation.	2008-09-22	4.7	CVE-2008-4160 BID FRSIRT SUNALERT SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
drupal -- talk	Cross-site scripting (XSS) vulnerability in the Talk module 5.x before 5.x-1.3 and 6.x before 6.x-1.5, a module for Drupal, allows remote authenticated users to inject arbitrary web script or HTML via a node title.	2008-09-24	3.5	CVE-2008-4152 CONFIRM
memht -- memht_portal	cron.php in MemHT Portal 3.9.0 and earlier allows remote attackers to obtain sensitive information via a direct request, which reveals the installation path in an error message.	2008-09-22	2.6	CVE-2008-4164 MILW0RM
opensolution -- quick.cms.lite	Cross-site scripting (XSS) vulnerability in admin.php in OpenSolution Quick.Cms.Lite 2.1 allows remote attackers to inject arbitrary web script or HTML via the query string.	2008-09-24	2.6	CVE-2008-4139 XF BID BUGTRAQ SECUNIA

Back to top