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**	
adaptcms -- adaptcms	SQL injection vulnerability in the "Check User" feature (includes/check_user.php) in AdaptCMS Lite and AdaptCMS Pro 1.3 allows remote attackers to execute arbitrary SQL commands via the user_name parameter.	2008-10-09	7.5	CV CO SE
adobe -- flash_player	Adobe Flash Player 8.0.39.0 and earlier, and 9.x up to 9.0.115.0, allows remote attackers to bypass the allowScriptAccess parameter setting via a crafted SWF file with unspecified "Filter evasion" manipulations.	2008-10-06	9.3	CV XF CO MI
ampjuke -- ampjuke	SQL injection vulnerability in index.php in AmpJuke 0.7.5 allows remote attackers to execute arbitrary SQL commands via the special parameter in a performerid action.	2008-10-09	7.5	CV BII SE MI

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
apache -- xerces-c++	The XML parser in Xerces-C++ before 3.0.0 allows context-dependent attackers to cause a denial of service (stack consumption and crash) via an XML schema definition with a large maxOccurs value, which triggers excessive memory consumption during validation of an XML file.	2008-10-07	7.8	CV BII
apple -- cups	The Hewlett-Packard Graphics Language (HPGL) filter in CUPS before 1.3.9 allows remote attackers to execute arbitrary code via crafted pen width and pen color opcodes that overwrite arbitrary memory.	2008-10-10	10.0	CV BII CO
apple -- mac_os_x apple -- mac_os_x_server	Buffer overflow in ColorSync in Mac OS X 10.4.11 and 10.5.5 allows remote attackers to cause a denial of service (application termination) and possibly execute arbitrary code via an image with a crafted ICC profile.	2008-10-10	9.3	CV BII AP
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in Finder in Mac OS X 10.5.5 allows user-assisted attackers to cause a denial of service (continuous termination and restart) via a crafted Desktop file that generates an error when producing its icon, related to an "error recovery issue."	2008-10-10	7.8	CV BII
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in the local IPC component in the EAPOLController plugin for configd (Networking component) in Mac OS X 10.4.11 and 10.5.5 allows local users to execute arbitrary code via unknown vectors.	2008-10-10	7.2	CV BII

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
apple -- mac_os_x apple -- mac_os_x_server	Buffer overflow in PSNormalizer in Mac OS X 10.4.11 and 10.5.5 allows remote attackers to cause a denial of service (application termination) and execute arbitrary code via a PostScript file with a crafted bounding box comment.	2008-10-10	9.3	CV BII AP
apple -- mac_os_x apple -- mac_os_x_server	Integer signedness error in QuickLook in Mac OS X 10.5.5 allows remote attackers to cause a denial of service (application termination) and execute arbitrary code via a crafted Microsoft Excel file that triggers an out-of-bounds memory access.	2008-10-10	10.0	CV BII
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in rlogind in the rlogin component in Mac OS X 10.4.11 and 10.5.5 applies hosts.equiv entries to root despite what is stated in documentation, which might allow remote attackers to bypass intended access restrictions.	2008-10-10	10.0	CV BII
apple -- mac_os_x_server	Weblog in Mac OS X Server 10.4.11 does not properly check an error condition when a weblog posting access control list is specified for a user that has multiple short names, which might allow attackers to bypass intended access restrictions.	2008-10-10	7.5	CV BII
asicms -- asicms	Multiple PHP remote file inclusion vulnerabilities in asiCMS alpha 0.208 allow remote attackers to execute arbitrary PHP code via a URL in the _ENV[asicms][path] parameter to (1) Association.php, (2) BigMath.php, (3)	2008-10-09	7.5	CV BII MI

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	DiffieHellman.php, (4) DumbStore.php, (5) Extension.php, (6) FileStore.php, (7) HMAC.php, (8) MemcachedStore.php, (9) Message.php, (10) Nonce.php, (11) SQLStore.php, (12) SReg.php, (13) TrustRoot.php, and (14) URINorm.php in classes/Auth/OpenID/; and (15) XRDS.php, (16) XRI.php and (17) XRIRes.php in classes/Auth/Yadis/.			
atarone -- atarone	Directory traversal vulnerability in ap-save.php in Atarone CMS 1.2.0 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the theme_chosen parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-07	10.0	CV XF BII SE
autodesk -- design_review autodesk -- dwf_viewer autodesk -- revit_architecture	Directory traversal vulnerability in the CExpressViewerControl class in the DWF Viewer ActiveX control (AdView.dll 9.0.0.96), as used in Revit Architecture 2009 SP2 and Autodesk Design Review 2009, allows remote attackers to overwrite arbitrary files via "..\" sequences in the argument to the SaveAS method.	2008-10-07	9.3	CV BU MI FR SE MI
autodesk -- design_review autodesk -- dwf_viewer autodesk -- revit_architecture	The UpdateEngine class in the LiveUpdate ActiveX control (LiveUpdate16.DLL 17.2.56), as used in Revit Architecture 2009 SP2 and Autodesk	2008-10-07	9.3	CV BU MI FR MI

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	Design Review 2009, allows remote attackers to execute arbitrary programs via the second argument to the ApplyPatch method.			
blue_coat_systems -- k9_web_protection	Blue Coat K9 Web Protection 4.0.230 Beta relies on client-side JavaScript as a protection mechanism, which allows remote attackers to bypass authentication and access the (1) summary, (2) detail, (3) overrides, and (4) pwemail pages by disabling JavaScript.	2008-10-09	7.5	CV XF BII FU MI
built2go -- real_estate_listings	SQL injection vulnerability in event_detail.php in Built2Go Real Estate Listings 1.5 allows remote attackers to execute arbitrary SQL commands via the event_id parameter.	2008-10-08	7.5	CV BII MI
cambridge_computer_corporation -- vxftpsrv	Buffer overflow in Cambridge Computer Corporation vxFtpSrv 2.0.3 allows remote attackers to cause a denial of service (crash and hang) and possibly execute arbitrary code via a long CWD request.	2008-10-06	9.0	CV BII MI
cisco -- unity	Unspecified vulnerability in Cisco Unity 4.x before 4.0ES161, 5.x before 5.0ES53, and 7.x before 7.0ES8, when using anonymous authentication, allows remote attackers to bypass authentication and read or modify system configuration parameters via unknown vectors.	2008-10-08	9.3	CV CIS
condor_project -- condor	Condor before 7.0.5 does not properly handle when the configuration specifies overlapping netmasks in allow or deny rules, which causes the rule to be ignored and	2008-10-08	7.2	CV SE BII RE RE FR

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	allows attackers to bypass intended access restrictions.			CC SE SE
customcms -- ccms	Multiple directory traversal vulnerabilities in CCMS 3.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the skin parameter to (1) index.php, (2) forums.php, (3) admin.php, (4) header.php, (5) pages/story.php and (6) pages/poll.php.	2008-10-09	10.0	CV BII MI
datafeedfile -- dff_framework_api	Multiple PHP remote file inclusion vulnerabilities in DataFeedFile (DFF) PHP Framework API allow remote attackers to execute arbitrary PHP code via a URL in the DFF_config[dir_include] parameter to (1) DFF_affiliate_client_API.php, (2) DFF_featured_prdt.func.php, (3) DFF_mer.func.php, (4) DFF_mer_prdt.func.php, (5) DFF_paging.func.php, (6) DFF_rss.func.php, and (7) DFF_sku.func.php in include/.	2008-10-08	10.0	CV MI
debian -- xsabre	A certain Debian patch to the run scripts for sabre (aka xsabre) 0.2.4b allows local users to delete or overwrite arbitrary files via a symlink attack on unspecified .tmp files.	2008-10-03	7.2	CV XF BII MI CO
debian -- feta	The to-upgrade plugin in feta 1.4.16 allows local users to overwrite arbitrary files via a symlink on a temporary file.	2008-10-03	7.2	CV BII DE SE CO
drupal -- brilliant_gallery	SQL injection vulnerability in Brilliant Gallery 5.x before 5.x-4.2, a module for Drupal, allows remote attackers to	2008-10-09	7.5	CV XF BII SE

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	execute arbitrary SQL commands via unspecified vectors, related to queries. NOTE: this might be the same issue as CVE-2008-4338.			CC
dspicture -- light_imaging_toolkit dspicture -- pro_imaging_sdk	The GdPicture (1) Light Imaging Toolkit 4.7.1 GdPicture4S.Imaging ActiveX control (gdpicture4s.ocx) 4.7.0.1 and (2) Pro Imaging SDK 5.7.1 GdPicturePro5S.Imaging ActiveX control (gdpicturepro5s.ocx) 5.7.0.1 allows remote attackers to create, overwrite, and modify arbitrary files via the SaveAsPDF method. NOTE: this issue might only be exploitable in limited environments or non-default browser settings. NOTE: this can be leveraged for remote code execution by accessing files using hcp:// URLs. NOTE: some of these details are obtained from third party information.	2008-10-06	9.3	CV BII
e-php_scripts -- b2b_trading_marketplace_script	SQL injection vulnerability in listings.php in E-Php B2B Trading Marketplace Script allows remote attackers to execute arbitrary SQL commands via the cid parameter in a product action.	2008-10-06	7.5	CV BII SE MI
ec-cube -- ec-cube	SQL injection vulnerability in EC-CUBE Ver2 2.1.2a and earlier, and Ver2 RC 2.3.0-rc1 and earlier, allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2008-10-10	7.5	CV CC
eset_software -- system_analyzer_tool	The SysInspector AntiStealth driver (esiasdrv.sys) 3.0.65535.0 in ESET System Analyzer Tool 1.1.1.0 allows	2008-10-06	7.2	CV BII MI MI

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	local users to execute arbitrary code via a certain IOCTL request to \Device\esiasdrv that overwrites a pointer.			
extrovert_software -- thyme	SQL injection vulnerability in pick_users.php in the groups module in eXtrovert Thyme 1.3 allows remote attackers to execute arbitrary SQL commands via the uname_search parameter. NOTE: some of these details are obtained from third party information.	2008-10-06	7.5	CV BII MI SE
fastpublish -- fastpublish_cms	Multiple SQL injection vulnerabilities in Fastpublish CMS 1.9.9.9.9 d (1.9999 d) allow remote attackers to execute arbitrary SQL commands via the (1) sprache parameter to index2.php and the (2) artikel parameter to index.php.	2008-10-09	7.5	CV BII MI SE
fastpublish -- fastpublish_cms	Multiple directory traversal vulnerabilities in Fastpublish CMS 1.9999 d allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the target parameter to (1) index2.php and (2) index.php.	2008-10-09	7.5	CV BII MI SE
force10 -- ftos freebsd -- freebsd juniper -- jnos netbsd -- netbsd openbsd -- openbsd windriver -- vxworks	The IPv6 Neighbor Discovery Protocol (NDP) implementation in (1) FreeBSD 6.3 through 7.1, (2) OpenBSD 4.2 and 4.3, (3) NetBSD, (4) Force10 FTOS before E7.7.1.1, (5) Juniper JUNOS, and (6) Wind River VxWorks 5.x through 6.4 does not validate the origin of Neighbor Discovery messages, which allows remote attackers to cause a denial of service (loss of connectivity) or read private	2008-10-03	9.3	CV CO CO CE MI XF BII OP OP FR FR FR SE FR SE

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	network traffic via a spoofed message that modifies the Forward Information Base (FIB).			SE SE
foss_gallery -- foss_gallery	Unrestricted file upload vulnerability in processFiles.php in FOSS Gallery Admin and FOSS Gallery Public 1.0 beta allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in the root directory.	2008-10-09	10.0	CV XF BII MI MI MI
freeradius -- freeradius	freeradius-dialupadmin in freeradius 2.0.4 allows local users to overwrite arbitrary files via a symlink attack on temporary files in (1) backup_radacct, (2) clean_radacct, (3) monthly_tot_stats, (4) tot_stats, and (5) truncate_radacct.	2008-10-07	7.2	CV BII MI SE MI CO
galerie -- galerie	SQL injection vulnerability in galerie.php in Galerie 3.2 allows remote attackers to execute arbitrary SQL commands via the pic parameter.	2008-10-09	7.5	CV XF BII MI
geccbblite -- geccbblite	SQL injection vulnerability in leggi.php in geccBBlite 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-09	7.5	CV BII MI
gnu -- ibackup	ibackup 2.27 allows local users to overwrite arbitrary files via a symlink attack on unspecified temporary files.	2008-10-07	7.2	CV MI MI CO
hammer-software -- metagauge	Directory traversal vulnerability in MetaGauge 1.0.0.17, and probably other versions before 1.0.3.38,	2008-10-07	7.8	CV BII

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	allows remote attackers to read arbitrary files via a "..\" (dot dot backslash) in the URL.			
hp -- oncplus	Unspecified vulnerability in NFS / ONCplus B.11.31_04 and earlier on HP-UX B.11.31 allows remote attackers to cause a denial of service via unknown attack vectors.	2008-10-07	7.8	CV HP
ibm -- lotus_quickr	Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) might allow attackers to cause a denial of service (system crash) via a "nonstandard URL argument" to the OpenDocument command. NOTE: due to lack of details from the vendor, it is not clear whether this is a vulnerability.	2008-10-09	7.8	CV XF BI FR CO SE
ibm -- lotus_quickr	Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) allows a place manager to "demote or delete a place superuser group" via unknown vectors.	2008-10-09	7.5	CV XF BI FR CO SE
ibm -- lotus_quickr	Unspecified vulnerability in IBM Lotus Quickr 8.1 before Fix pack 1 (8.1.0.1) allows editors to delete pages that were created by a different author via unknown vectors.	2008-10-09	7.5	CV XF BI FR CO SE
ip_reg -- ip_reg	SQL injection vulnerability in login.php in IP Reg 0.4 and earlier allows remote attackers to execute arbitrary SQL commands via the user_name parameter.	2008-10-09	7.5	CV XF BI MI
iseemedia -- lpviewer mgi_software -- lpviewer roxio -- lpviewer	Multiple stack-based buffer overflows in MGI Software LPViewer ActiveX control (LPControl.dll), as acquired by Roxio and iseemedia, allow remote attackers to	2008-10-07	9.3	CV CE XF BI FR SE

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	execute arbitrary code via the (1) url, (2) toolbar, and (3) enableZoomPastMax methods.			
jesse-web -- jmweb_mp3_music_audio_search_and_download_script	Multiple directory traversal vulnerabilities in JMweb MP3 Music Audio Search and Download Script allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the src parameter to (1) listen.php and (2) download.php.	2008-10-09	7.5	CV BII MI SE
jim_trocki -- mon	alert.d/test.alert in mon 0.99.2 allows local users to overwrite arbitrary files via a symlink attack on the test.alert.log temporary file.	2008-10-07	7.2	CV MI CO
libvirt -- libvirt	libvirt 0.3.3 relies on files located under subdirectories of /local/domain in xenstore despite lack of protection against modification by Xen guest virtual machines, which allows guest OS users to have an unspecified impact, as demonstrated by writing to (1) the text console (console/tty) or (2) the VNC port for the graphical framebuffer.	2008-10-03	7.2	CV CO MI CO SE FR SE MI MI MI
lighttpd -- lighttpd	lighttpd before 1.4.20 compares URIs to patterns in the (1) url.redirect and (2) url.rewrite configuration settings before performing URL decoding, which might allow remote attackers to bypass intended access restrictions, and obtain sensitive information or possibly modify data.	2008-10-03	7.5	CV CO
lighttpd -- lighttpd	mod_userdir in lighttpd before 1.4.20, when a case-insensitive operating system or filesystem is used, performs case-sensitive	2008-10-03	7.8	CV CO CO CO

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	comparisons on filename components in configuration options, which might allow remote attackers to bypass intended access restrictions, as demonstrated by a request for a .PHP file when there is a configuration rule for .php files.			
mirc -- mirc	Stack-based buffer overflow in mIRC 6.34 allows remote attackers to execute arbitrary code via a long hostname in a PRIVMSG message.	2008-10-06	9.3	CV XF BII MI MI FR SE
numark -- cue	Stack-based buffer overflow in Numark CUE 5.0 rev2 allows user-assisted attackers to cause a denial of service (application crash) or execute arbitrary code via an M3U playlist file that contains a long absolute pathname.	2008-10-06	9.3	CV XF BII MI FR
phlatline -- personal_information_manager	Directory traversal vulnerability in notes.php in Phlatline's Personal Information Manager (pPIM) 1.01 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the id parameter in an edit action.	2008-10-09	7.5	CV BII MI
php-fusion -- world_of_warcraft_tracker_infusion_module	SQL injection vulnerability in thisraidprogress.php in the World of Warcraft tracker infusion (raidtracker_panel) module 2.0 for PHP-Fusion allows remote attackers to execute arbitrary SQL commands via the INFO_RAID_ID parameter.	2008-10-09	7.5	CV BII MI
php-fusion -- recepies_module	SQL injection vulnerability in recept.php in the Recepies (Recept) module 1.1 for PHP-Fusion allows remote	2008-10-09	7.5	CV BII MI SE

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	attackers to execute arbitrary SQL commands via the kat_id parameter in a kategorier action. NOTE: some of these details are obtained from third party information.			
php_web_explorer -- php_web_explorer_lite	Multiple directory traversal vulnerabilities in PHP Web Explorer 0.99b and earlier allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) refer parameter to main.php and the (2) file parameter to edit.php.	2008-10-08	9.3	CV XF BII BU
phpautos -- phpautos	SQL injection vulnerability in searchresults.php in PHP Autos 2.9.1 allows remote attackers to execute arbitrary SQL commands via the catid parameter.	2008-10-08	7.5	CV BII MI SE
rmsoft -- minishop_module	SQL injection vulnerability in search.php in the RMSOFT MiniShop module 1.0 for Xoops might allow remote attackers to execute arbitrary SQL commands via the itemsxpag parameter.	2008-10-03	7.5	CV MI
select_development_solutions -- php_auto_dealer	SQL injection vulnerability in view_cat.php in PHP Auto Dealer 2.7 allows remote attackers to execute arbitrary SQL commands via the v_cat parameter.	2008-10-08	7.5	CV MI SE
select_development_solutions -- php_realtor	SQL injection vulnerability in view_cat.php in PHP Realtor 1.5 allows remote attackers to execute arbitrary SQL commands via the v_cat parameter.	2008-10-08	7.5	CV MI SE
serv-u -- serv-u_file_server	Directory traversal vulnerability in the FTP server in Serv-U 7.3, and 7.2.0.1 and earlier, allows remote authenticated users to	2008-10-08	9.0	CV FR

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
	overwrite or create arbitrary files via a ..\ (dot dot backslash) in the RNTO command.			
sympa -- sympa	sympa.pl in sympa 5.3.4 allows local users to overwrite arbitrary files via a symlink attack on a temporary file. NOTE: wwsympa.fcgi was also reported, but the issue occurred in a dead function, so it is not a vulnerability.	2008-10-07	7.2	CV MI CO
tonec_inc. -- internet_download_manager	Stack-based buffer overflow in the file parsing function in Tonec Internet Download Manager, possibly 5.14 and earlier, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted AppleDouble file containing a long string. NOTE: this is probably a different vulnerability than CVE-2005-2210.	2008-10-09	7.8	CV XF BII MI
torrenttrader -- torrenttrader	SQL injection vulnerability in completed-advance.php in TorrentTrader Classic 1.08 and 1.04 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-08	7.5	CV BII MI SE
trend_micro -- officescan	Multiple buffer overflows in CGI modules in the server in Trend Micro OfficeScan 8.0 SP1 before build 2439 and 8.0 SP1 Patch 1 before build 3087 allow remote attackers to execute arbitrary code via unspecified vectors.	2008-10-03	10.0	CV BII
v-webmail -- v-webmail	SQL injection vulnerability in login.php in V-webmail 1.5.0 might allow remote attackers to execute arbitrary SQL commands via the username parameter.	2008-10-07	7.5	CV OS MI

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
vastal_i-tech -- mmorpg_zone	SQL injection vulnerability in game.php in Vastal I-Tech MMORPG Zone allows remote attackers to execute arbitrary SQL commands via the game_id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- dating_zone	SQL injection vulnerability in advanced_search_results.php in Vastal I-Tech Dating Zone, possibly 0.9.9, allows remote attackers to execute arbitrary SQL commands via the fage parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- visa_zone	SQL injection vulnerability in view_news.php in Vastal I-Tech Visa Zone allows remote attackers to execute arbitrary SQL commands via the news_id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- jobs_zone	SQL injection vulnerability in view_news.php in Vastal I-Tech Jobs Zone allows remote attackers to execute arbitrary SQL commands via the news_id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- mag_zone	SQL injection vulnerability in view_mags.php in Vastal I-Tech Mag Zone allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- dvd_zone	SQL injection vulnerability in view_mags.php in Vastal I-Tech DVD Zone allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- cosmetics_zone	SQL injection vulnerability in view_products_cat.php in Vastal I-Tech Cosmetics Zone allows remote attackers to execute arbitrary SQL commands via the cat_id parameter.	2008-10-06	7.5	CV XF BII MI SE

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	
vastal_i-tech -- toner_cart	SQL injection vulnerability in show_series_ink.php in Vastal I-Tech Toner Cart allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- share_zone	SQL injection vulnerability in view_news.php in Vastal I-Tech Share Zone allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-06	7.5	CV XF BII MI
vastal_i-tech -- freelance_zone	SQL injection vulnerability in view_cresume.php in Vastal I-Tech Freelance Zone allows remote attackers to execute arbitrary SQL commands via the coder_id parameter.	2008-10-06	7.5	CV XF BII MI
yerba -- yerba	Directory traversal vulnerability in index.php in SAC.php (SACphp), as used in Yerba 6.3 and earlier, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the mod parameter.	2008-10-07	10.0	CV BII BU MI FR
yourownbux -- yourownbux	SQL injection vulnerability in referrals.php in YourOwnBux 4.0 allows remote attackers to execute arbitrary SQL commands via the usNick cookie.	2008-10-08	7.5	CV BII MI

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
asp/ms access	ASP/MS Access Shoutbox, probably 1.1 beta, stores db/shoutdb.mdb under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request.	2008-10-09	5.0	CVE-2008-4512 BUGTRAQ

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- flash_player	The Settings Manager in Adobe Flash Player 9.0.124.0 and earlier allows remote attackers to cause victims to unknowingly click on a link or dialog via access control dialogs disguised as normal graphical elements, as demonstrated by hijacking the camera or microphone, and related to "clickjacking."	2008-10-09	6.8	CVE-2008-4503 XF SECTRACK BID FRSIRT CONFIRM SECUNIA MISC MISC
apache_friends -- xampp	Cross-site scripting (XSS) vulnerability in adodb.php in XAMPP for Windows 1.6.8 allows remote attackers to inject arbitrary web script or HTML via the (1) dbserver, (2) host, (3) user, (4) password, (5) database, and (6) table parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-06	4.3	CVE-2008-4450 XF BID SECUNIA
apple -- mail	Apple Mail.app 3.5 on Mac OS X, when "Store draft messages on the server" is enabled, stores draft copies of S/MIME email in plaintext on the email server, which allows server owners and remote man-in-the-middle attackers to read sensitive mail.	2008-10-08	5.0	CVE-2008-4491 XF BID BUGTRAQ MISC MISC
apple -- mac_os_x	The Postfix configuration file in Mac OS X 10.5.5 causes Postfix to be network-accessible when mail is sent from a local command-line tool, which allows remote attackers to send mail to local Mac OS X users.	2008-10-10	6.8	CVE-2008-3646 BID APPLE
apple -- mac_os_x apple -- mac_os_x_server	Unspecified vulnerability in Script Editor in Mac OS X 10.4.11 and 10.5.5 allows local users to cause the scripting dictionary to be written to arbitrary locations, related to an "insecure file operation" on temporary files.	2008-10-10	4.6	CVE-2008-4214 BID APPLE

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
atarone -- atarone	SQL injection vulnerability in ap-save.php in Atarone CMS 1.2.0 allows remote attackers to execute arbitrary SQL commands via the (1) site_name, (2) email, (3) theme_chosen, (4) hp, (5) c_meta, (6) id, and (7) c_js parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-07	6.8	CVE-2008-4487 XF BID SECUNIA
atarone -- atarone	Cross-site scripting (XSS) vulnerability in ap-pages.php in Atarone CMS 1.2.0 allows remote attackers to inject arbitrary web script or HTML via the (1) name and (2) id parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-07	4.3	CVE-2008-4488 XF BID SECUNIA
autonessus -- autonessus	Cross-site scripting (XSS) vulnerability in bulk_update.pl in AutoNessus before 1.2.2 allows remote attackers to inject arbitrary web script or HTML via the remark parameter.	2008-10-09	4.3	CVE-2008-4520 BID CONFIRM
bluecoat -- security_gateway_os	Cross-site scripting (XSS) vulnerability in the ICAP patience page in Blue Coat Security Gateway OS (SGOS) 4.2 before 4.2.9, 5.2 before 5.2.5, and 5.3 before 5.3.1.7 allows remote attackers to inject arbitrary web script or HTML via the URL.	2008-10-07	4.3	CVE-2008-4485 SECTRACK BID FRSIRT CONFIRM SECUNIA BUGTRAQ BUGTRAQ
condor_project -- condor	Unspecified vulnerability in Condor before 7.0.5 allows attackers to execute jobs as other users via unknown vectors.	2008-10-08	4.6	CVE-2008-3826 SECTRACK BID REDHAT REDHAT FRSIRT CONFIRM SECUNIA SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
condor_project -- condor	Stack-based buffer overflow in the condor_ schedd daemon in Condor before 7.0.5 allows attackers to cause a denial of service (crash) and possibly execute arbitrary code via unknown vectors.	2008-10-08	4.6	CVE-2008-3828 SECTRACK BID REDHAT REDHAT FRSIRT CONFIRM SECUNIA SECUNIA
condor_project -- condor	Unspecified vulnerability in the condor_ schedd daemon in Condor before 7.0.5 allows attackers to cause a denial of service (crash) via unknown vectors.	2008-10-08	5.0	CVE-2008-3829 SECTRACK BID REDHAT REDHAT FRSIRT CONFIRM SECUNIA SECUNIA
crux_software -- gallery	Directory traversal vulnerability in index.php in Crux Gallery 1.32 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the theme parameter.	2008-10-07	6.8	CVE-2008-4483 BID MILW0RM SECUNIA
crux_software -- gallery	main.php in Crux Gallery 1.32 and earlier assumes that the user is an administrator if the name parameter is not "users", which allows remote attackers to gain administrative access by setting the name parameter to "users", as demonstrated via index.php.	2008-10-07	6.8	CVE-2008-4484 BID BUGTRAQ VIM SECUNIA MILW0RM
drupal -- brilliant_gallery	Cross-site scripting (XSS) vulnerability in Brilliant Gallery 5.x before 5.x-4.2, a module for Drupal, allows remote authenticated users with permissions to inject arbitrary web script or HTML via unspecified vectors related to posting of answers.	2008-10-09	4.3	CVE-2008-4530 CONFIRM
ec-cube -- ec-cube	Cross-site scripting (XSS) vulnerability in EC-CUBE Ver2 2.1.2a and earlier, EC-CUBE	2008-10-10	4.3	CVE-2008-4535 MISC

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Ver2 Beta(RC) 2.2.0-beta and earlier, and EC-CUBE Community Edition Nighly-Build r17623 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4536 and CVE-2008-4537.			
ec-cube -- ec-cube	Cross-site scripting (XSS) vulnerability in EC-CUBE Ver1 1.4.6 and earlier, Ver1 Beta 1.5.0-beta and earlier, Ver2 2.1.2a and earlier, Ver2 Beta(RC) 2.2.0-beta and earlier, Community Edition 1.3.4 and earlier, and Community Edition Nightly-Build r17319 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4535 and CVE-2008-4537.	2008-10-10	4.3	CVE-2008-4536 MISC SECUNIA
ec-cube -- ec-cube	Cross-site scripting (XSS) vulnerability in EC-CUBE Ver1 1.4.6 and earlier, Ver1 Beta 1.5.0-beta and earlier, Ver2 2.1.2a and earlier, Ver2 Beta(RC) 2.1.1-beta and earlier, Community Edition 1.3.4 and earlier, and Community Edition Nightly-Build r17336 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2008-4535 and CVE-2008-4536.	2008-10-10	4.3	CVE-2008-4537 MISC
gentoo -- portage	Multiple untrusted search path vulnerabilities in Portage before 2.1.4.5 include the current working directory in the Python search path, which allows local users to execute arbitrary code via a modified Python module that is loaded by the (1) ys-apps/portage, (2) net-mail/fetchmail, (3)	2008-10-10	6.9	CVE-2008-4394 BID GENTOO

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	app-editors/leo ebuilds, and other ebuilds.			
herosoft -- hero_dvd_player	Heap-based buffer overflow in Mplayer.exe in Herosoft Inc. Hero DVD Player 3.0.8 allows user-assisted remote attackers to execute arbitrary code via an M3u file with a "long entry." NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-09	6.8	CVE-2008-4504 BID SECUNIA
katan -- web_server	Cross-site scripting (XSS) vulnerability in Kantan WEB Server 1.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2008-10-10	4.3	CVE-2008-4533 BID
konqueror -- konqueror	The HTML parser in KDE Konqueror 3.5.9 allows remote attackers to cause a denial of service (application crash) via a font tag with a long color value, which triggers an assertion error.	2008-10-09	5.0	CVE-2008-4514 BID MILW0RM
linux -- kernel	The generic_file_splice_write function in fs/splice.c in the Linux kernel before 2.6.19 does not properly strip setuid and setgid bits when there is a write to a file, which allows local users to gain the privileges of a different group, and obtain sensitive information or possibly have unspecified other impact, by splicing into an inode in order to create an executable file in a setgid directory, a different vulnerability than CVE-2008-4210.	2008-10-03	4.9	CVE-2008-3833 CONFIRM BID CONFIRM MLIST CONFIRM
linux -- kernel	The vmi_write_ldt_entry function in arch/x86/kernel/vmi_32.c in the Virtual Machine Interface (VMI) in the Linux kernel 2.6.26.5 invokes write_idt_entry where write_ldt_entry was intended, which allows local users to cause a denial of service (persistent	2008-10-03	4.9	CVE-2008-4410 XF BID MLIST SECUNIA CONFIRM

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	application failure) via crafted function calls, related to the Java Runtime Environment (JRE) experiencing improper LDT selector state, a different vulnerability than CVE-2008-3247.			
linux -- kernel	The sctp_auth_ep_set_hmacs function in net/sctp/auth.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.26.4, when the SCTP-AUTH extension is enabled, does not verify that the identifier index is within the bounds established by SCTP_AUTH_HMAC_ID_MAX, which allows local users to obtain sensitive information via a crafted SCTP_HMAC_IDENT IOCTL request involving the sctp_getsockopt function, a different vulnerability than CVE-2008-4113.	2008-10-06	4.7	CVE-2008-4445 SECTRACK REDHAT MLIST MLIST MLIST MLIST CONFIRM SECUNIA MLIST MLIST CONFIRM
maxiscript -- website_directory	Cross-site scripting (XSS) vulnerability in index.php in MaxiScript Website Directory allows remote attackers to inject arbitrary web script or HTML via the keyword parameter in a search action.	2008-10-09	4.3	CVE-2008-4532 XF BID BUGTRAQ SECUNIA
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in MediaWiki 1.13.1, 1.12.0, and possibly other versions before 1.13.2 allows remote attackers to inject arbitrary web script or HTML via the useskin parameter to an unspecified component.	2008-10-03	4.3	CVE-2008-4408 FEDORA FEDORA XF BID FRSIRT CONFIRM CONFIRM SECUNIA SECUNIA MLIST MLIST
memht -- memht_portal	SQL injection vulnerability in inc/inc_statistics.php in MemHT Portal 3.9.0 and earlier, when	2008-10-06	6.8	CVE-2008-4457 BID CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via a stats_res cookie to index.php.			
microsoft -- digital_image	Microsoft PicturePusher ActiveX control (PipPPush.DLL 7.00.0709), as used in Microsoft Digital Image 2006 Starter Edition, allows remote attackers to force the upload of arbitrary files by using the AddString and Post methods and a modified PostURL to construct an HTTP POST request. NOTE: this issue might only be exploitable in limited environments or non-default browser settings.	2008-10-08	6.8	CVE-2008-4493 XF SECTRACK BID MILW0RM
microsoft -- windows-nt	Microsoft Windows Vista Home and Ultimate Edition SP1 and earlier allows local users to cause a denial of service (page fault and system crash) via multiple attempts to access a virtual address in a PAGE_NOACCESS memory page.	2008-10-09	4.9	CVE-2008-4510 BID MILW0RM SECUNIA
mysql_quick_admin -- mysql_quick_admin	Directory traversal vulnerability in EKINdesigns MySQL Quick Admin 1.5.5 allows remote attackers to read and execute arbitrary files via a .. (dot dot) in the lang parameter to actions.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-06	6.8	CVE-2008-4454 SECUNIA
mysql_quick_admin -- mysql_quick_admin	Directory traversal vulnerability in index.php in EKINdesigns MySQL Quick Admin 1.5.5 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to read and execute arbitrary files via a .. (dot dot) in the language cookie.	2008-10-06	6.8	CVE-2008-4455 XF BID SECUNIA MILW0RM
nucleus_cms -- nucleus	Cross-site scripting (XSS) vulnerability in Nucleus EUC-JP 3.31 SP1 and earlier allows	2008-10-06	4.3	CVE-2008-4446 XF BID

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	remote attackers to inject arbitrary web script or HTML via unspecified vectors.			SECUNIA JVNDB JVN CONFIRM CONFIRM
phorum -- phorum	Cross-site scripting (XSS) vulnerability in BBcode API module in Phorum 5.2.8 allows remote attackers to inject arbitrary web script or HTML via nested BBcode image tags.	2008-10-09	4.3	CVE-2008-4513 XF BID CONFIRM MISC
phpabook -- phpabook	Directory traversal vulnerability in config.inc.php in phpAbook 0.8.8b and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the userInfo cookie.	2008-10-07	5.1	CVE-2008-4490 XF BID MILW0RM
positive_software -- h-sphere	Cross-site scripting (XSS) vulnerability in actions.php in Positive Software H-Sphere WebShell 4.3.10 allows remote attackers to inject arbitrary web script or HTML via (1) the fn parameter during a dload action, (2) the fld parameter during a search action, and (3) the tab parameter during a sysinfo action.	2008-10-06	4.3	CVE-2008-4447 XF BID MISC
positive_software -- h-sphere	Cross-site request forgery (CSRF) vulnerability in actions.php in Positive Software H-Sphere WebShell 4.3.10 allows remote attackers to perform unauthorized actions as an administrator, including file deletion and creation, via a link or IMG tag to the (1) overkill, (2) futils, or (3) edit actions.	2008-10-06	6.8	CVE-2008-4448 XF MISC
redhat -- enterprise_linux redhat -- enterprise_linux_desktop	pam_krb5 2.2.14 in Red Hat Enterprise Linux (RHEL) 5 and earlier, when the existing_ticket option is enabled, uses incorrect privileges when reading a Kerberos credential cache, which allows local users to gain	2008-10-03	4.4	CVE-2008-3825 FEDORA FEDORA CONFIRM XF SECTRACK BID

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	privileges by setting the KRB5CCNAME environment variable to an arbitrary cache filename and running the (1) su or (2) sudo program. NOTE: there may be a related vector involving sshd that has limited relevance.			REDHAT MANDRIVA SECUNIA SECUNIA SECUNIA
redhat -- fedora	A certain Fedora patch for the utrace subsystem in the Linux kernel before 2.6.26.5-28 on Fedora 8, and before 2.6.26.5-45 on Fedora 9, allows local users to cause a denial of service (NULL pointer dereference and system crash or hang) via a call to the utrace_control function.	2008-10-03	4.9	CVE-2008-3832 CONFIRM XF BID MLIST MISC
redmine -- redmine	Cross-site scripting (XSS) vulnerability in Redmine 0.7.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2008-10-07	4.3	CVE-2008-4481 BID
serv-u -- serv-u_file_server	Serv-U 7.3, and 7.2.0.1 and earlier, allows remote authenticated users to cause a denial of service (CPU consumption) via a crafted stou command, probably related to MS-DOS device names, as demonstrated using "con:1".	2008-10-08	6.8	CVE-2008-4500 BID MILW0RM FRSIRT SECUNIA
todd_woolums -- asp_news_management	Todd Woolums ASP News Management, possibly 2.21, stores db/news.mdb under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request.	2008-10-09	5.0	CVE-2008-4511 BUGTRAQ
trend_micro -- officescan trend_micro -- worry_free_business_security	Directory traversal vulnerability in the UpdateAgent function in TmListen.exe in the OfficeScanNT Listener service in the client in Trend Micro OfficeScan 7.3 Patch 4 build 1367 and other builds before 1372, OfficeScan 8.0 SP1 before build 1222, OfficeScan 8.0 SP1 Patch 1	2008-10-03	5.0	CVE-2008-2439 CONFIRM CONFIRM CONFIRM CONFIRM FRSIRT SECUNIA SECUNIA

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	before build 3087, and Worry-Free Business Security 5.0 before build 1220 allows remote attackers to read arbitrary files via directory traversal sequences in an HTTP request. NOTE: some of these details are obtained from third party information.			
trend_micro -- officescan	The CGI modules in the server in Trend Micro OfficeScan 8.0 SP1 before build 2439 and 8.0 SP1 Patch 1 before build 3087 allow remote attackers to cause a denial of service (NULL pointer dereference and child process crash) via crafted HTTP headers, related to the "error handling mechanism."	2008-10-03	5.0	CVE-2008-4403 CONFIRM CONFIRM SECTRACK BID FRSIRT SECUNIA
v-webmail -- v-webmail	V-webmail 1.5.0 allows remote attackers to obtain sensitive information via (1) malformed input in the login page (includes/local.hooks.php) and (2) an invalid session ID, which reveals the installation path in an error message.	2008-10-07	5.0	CVE-2008-3060 OSVDB OSVDB MISC
v-webmail -- v-webmail	Open redirect vulnerability in redirect.php in V-webmail 1.5.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the to parameter.	2008-10-07	4.3	CVE-2008-3061 OSVDB MISC
verisign -- kontiki_delivery_management_system	Cross-site scripting (XSS) vulnerability in VeriSign Kontiki Delivery Management System (DMS) 5.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the action parameter to zodiac/servlet/zodiac.	2008-10-07	4.3	CVE-2008-4393 MISC FULLDISC
vim -- vim	Heap-based buffer overflow in the mch_expand_wildcards function in os_unix.c in Vim 6.2 and 6.3 allows user-assisted attackers to execute arbitrary code via shell metacharacters in filenames, as	2008-10-10	6.8	CVE-2008-3432 BID APPLE

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	demonstrated by the netrw.v3 test case.			
vmware -- esx vmware -- player vmware -- server vmware -- workstation	The CPU hardware emulation for 64-bit guest operating systems in VMware Workstation 6.0.x before 6.0.5 build 109488 and 5.x before 5.5.8 build 108000; Player 2.0.x before 2.0.5 build 109488 and 1.x before 1.0.8; Server 1.x before 1.0.7 build 108231; and ESX 2.5.4 through 3.5 allows authenticated guest OS users to gain additional guest OS privileges by triggering an exception that causes the virtual CPU to perform an indirect jump to a non-canonical address.	2008-10-06	6.8	CVE-2008-4279 CONFIRM
xmlsoft -- libxml2	libxml2 2.7.0 and 2.7.1 does not properly handle "predefined entities definitions" in entities, which allows context-dependent attackers to cause a denial of service (memory consumption and application crash), as demonstrated by use of xmllint on a certain XML document, a different vulnerability than CVE-2003-1564 and CVE-2008-3281.	2008-10-03	5.0	CVE-2008-4409 FEDORA FEDORA BID SECUNIA SECUNIA MLIST CONFIRM

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
freedesktop -- dbus freedesktop -- dbus1.0 freedesktop -- dbus1.1.0	The dbus_signature_validate function in the D-bus library (libdbus) before 1.2.4 allows remote attackers to cause a denial of service (application abort) via a message containing a malformed signature, which triggers a failed assertion error.	2008-10-07	2.1	CVE-2008-3834 CONFIRM CONFIRM XF BID FRSIRT CONFIRM SECUNIA
mysql -- mysql	Cross-site scripting (XSS) vulnerability in the command-line client in MySQL 5.0.26 through	2008-10-06	2.6	CVE-2008-4456 BUGTRAQ

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	5.0.45, when the --html option is enabled, allows attackers to inject arbitrary web script or HTML by placing it in a database cell, which might be accessed by this client when composing an HTML document.			BUGTRAQ BUGTRAQ MISC SECUNIA CONFIRM
vmware -- virtualcenter	VMware VirtualCenter 2.5 before Update 3 build 119838 on Windows displays a user's password in cleartext when the password contains unspecified special characters, which allows physically proximate attackers to steal the password.	2008-10-06	2.1	CVE-2008-4278 CONFIRM
Back to top				