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

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

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

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

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
6rbscript -- 6rbscript	SQL injection vulnerability in cat.php in 6rbScript allows remote attackers to execute arbitrary SQL commands via the CatID parameter.	2008-09-30	7.5	CVE-2008-4344 XF BID MISC
atomic_photo_album -- atomic_photo_album	SQL injection vulnerability in album.php in Atomic Photo Album (APA) 1.1.0pre4 allows remote attackers to execute arbitrary SQL commands via the apa_album_ID parameter.	2008-09-30	7.5	CVE-2008-4335 BID MILW0RM
availscript -- availscript_photo_album	SQL injection vulnerability in pics.php in Availscript Photo Album allows remote attackers to execute arbitrary SQL commands via the sid parameter.	2008-10-01	7.5	CVE-2008-4369 BID MILW0RM
availscript -- availscript_article_script	SQL injection vulnerability in articles.php in AvailScript Article Script allows remote attackers to execute arbitrary SQL commands via the aIDS parameter.	2008-10-01	7.5	CVE-2008-4371 BID MILW0RM
availscript -- availscript_jobs_portal_script	SQL injection vulnerability in job_seeker/applynow.php in AvailScript Job Portal Script allows remote attackers to execute arbitrary SQL commands via the jid parameter.	2008-10-01	7.5	CVE-2008-4373 BID MILW0RM
availscript -- availscript_classmate_script	SQL injection vulnerability in viewprofile.php in Availscript Classmate Script allows remote attackers to execute arbitrary SQL commands via the p parameter.	2008-10-01	7.5	CVE-2008-4375 BID MILW0RM
burnaware_technologies -- burnaware impressum -- cdburnerxp numedia_soft -- numedia_dvd_burning_sdk	NuMedia Soft NMS DVD Burning SDK Activex NMSDVDX.DVDEngineX.1 ActiveX control (NMSDVDX.dll) 1.013C and earlier, as used in CDBurnerXP 4.2.1.976, BurnAware 2.1.3, and possibly other products, allows remote attackers to overwrite and create arbitrary files via calls to the	2008-09-30	9.3	CVE-2008-4342 XF MISC BID MILW0RM FRSIRT

	EnableLog and LogMessage methods. NOTE: this issue might only be exploitable in limited environments or non-default browser settings. NOTE: some of these details are obtained from third party information. NOTE: this can be leveraged for remote code execution by accessing files using hcp:// URLs.			SECUNIA SECUNIA SECUNIA MISC
cannot -- php_infoboard	SQL injection vulnerability in the showjavatopic function in func.php in PHP infoBoard V.7 Plus allows remote attackers to execute arbitrary SQL commands via the idcat parameter to showtopic.php.	2008-09-30	7.5	CVE-2008-4332 BID MILW0RM
cannot -- php_infoboard	PHP infoBoard V.7 Plus allows remote attackers to bypass authentication and gain administrative access by setting the infouser cookie to 1.	2008-09-30	7.5	CVE-2008-4334 BID MILW0RM
chilkat_software -- chilkat_xml_activex_control	The Chilkat XML ChilkatUtil.CkData.1 ActiveX control (ChilkatUtil.dll) 3.0.3.0 and earlier allows remote attackers to create, overwrite, and modify arbitrary files for execution via a call to the (1) SaveToFile, (2) SaveToTempFile, or (3) AppendBinary 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.	2008-09-30	9.3	CVE-2008-4343 XF MISC BID MILW0RM SECUNIA
cisco -- ios	The SERVICE.DNS signature engine in the Intrusion Prevention System (IPS) in Cisco IOS 12.3 and 12.4 allows remote attackers to cause a denial of service (device crash or hang) via network traffic that triggers unspecified IPS signatures, a different vulnerability than CVE-2008-1447.	2008-09-26	7.8	CVE-2008-2739 CISCO
cisco -- ios	Cisco IOS 12.4 allows remote attackers to cause a denial of service (device crash) via a normal, properly formed SSL packet that occurs during termination of an SSL session.	2008-09-26	7.8	CVE-2008-3798 CISCO
cisco -- unified_callmanager cisco -- unified_communications_manager cisco -- ios	Unspecified vulnerability in the Session Initiation Protocol (SIP) implementation in Cisco IOS 12.2 through 12.4 and Unified Communications Manager 4.1 through 6.1, when VoIP is configured, allows remote attackers to cause a denial of service (device or process reload) via unspecified valid SIP messages, aka Cisco Bug ID CSCsu38644, a different vulnerability than CVE-2008-3801 and CVE-2008-3802.	2008-09-26	7.1	CVE-2008-3800 CISCO CISCO
cisco -- ios	Unspecified vulnerability in the Session Initiation Protocol (SIP) implementation in Cisco IOS 12.2 through 12.4, when VoIP is configured, allows remote attackers to cause a denial of service (device reload) via unspecified valid SIP messages, aka Cisco bug ID CSCsk42759, a different vulnerability than CVE-2008-3800 and CVE-2008-3801.	2008-09-26	7.1	CVE-2008-3802 CISCO
cisco -- ios	Cisco IOS 12.0 through 12.4 on Gigabit Switch Router (GSR) devices (aka 12000 Series routers) allows remote attackers to cause a denial of service	2008-09-26	7.1	CVE-2008-3809 CISCO

	(device crash) via a malformed Protocol Independent Multicast (PIM) packet.			
cmsbuzz -- cms_buzz	SQL injection vulnerability in index.php in CMS Buzz allows remote attackers to execute arbitrary SQL commands via the id parameter in a playgame action.	2008-10-01	7.5	CVE-2008-4374 BID MILW0RM SECUNIA
creative_mind -- creator_cms	SQL injection vulnerability in index.asp in Creative Mind Creator CMS 5.0 allows remote attackers to execute arbitrary SQL commands via the sideid parameter.	2008-10-01	7.5	CVE-2008-4377 XF BID MILW0RM
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	CVE-2008-4406 MLIST CONFIRM
deslock -- deslock	DLMFENC.sys 1.0.0.28 in DESlock+ 3.2.7 allows local users to cause a denial of service (system crash) or potentially execute arbitrary code via a certain DLMFENC_IOCTL request to \\.\DLKPFSD_Device that overwrites a pointer, probably related to use of the ProbeForRead function when ProbeForWrite was intended.	2008-09-30	7.2	CVE-2008-4363 MILW0RM FRSIRT SECUNIA MISC
easyrealtorpro -- easyrealtorpro	SQL injection vulnerability in site_search.php in EasyRealtorPRO 2008 allows remote attackers to execute arbitrary SQL commands via the (1) item, (2) search_ordermethod, and (3) search_order parameters.	2008-09-30	7.5	CVE-2008-4328 BID BUGTRAQ MISC
flashget -- flashget_ftp	Buffer overflow in FlashGet (formerly JetCar) FTP 1.9 allows remote FTP servers to execute arbitrary code via a long response to the PWD command.	2008-09-29	9.3	CVE-2008-4321 BID MILW0RM SECUNIA
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 network traffic via a spoofed message that modifies the Forward Information Base (FIB).	2008-10-03	9.3	CVE-2008-2476 CONFIRM CONFIRM CERT-VN MISC XF BID OPENBSD OPENBSD SECTRACK FREEBSD SECUNIA SECUNIA
hp -- insight_diagnostics	Unspecified vulnerability in HP Insight Diagnostics before 7.9.1.2402 allows remote attackers to read arbitrary files via unknown vectors.	2008-10-02	7.8	CVE-2008-3542 XF BID HP
ibm -- zseries	The IPv6 Neighbor Discovery Protocol (NDP) implementation on IBM zSeries servers 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 network traffic via a spoofed message that modifies the Forward Information Base (FIB), a	2008-10-03	10.0	CVE-2008-4404 MISC CERT-VN

	related issue to CVE-2008-2476.			
jasper_project -- jasper	Multiple integer overflows in JasPer 1.900.1 might allow context-dependent attackers to have an unknown impact via a crafted image file, related to integer multiplication for memory allocation.	2008-10-02	9.3	CVE-2008-3520 BID MISC
jasper_project -- jasper	The jas_stream_tmpfile function in libjasper/base/jas_stream.c in JasPer 1.900.1 allows local users to overwrite arbitrary files via a symlink attack on a tmp.XXXXXXXXXX temporary file.	2008-10-02	7.2	CVE-2008-3521 BID CONFIRM CONFIRM
jasper_project -- jasper	Buffer overflow in the jas_stream_printf function in libjasper/base/jas_stream.c in JasPer 1.900.1 might allow context-dependent attackers to have an unknown impact via vectors related to the mif_hdr_put function and use of vsprintf.	2008-10-02	10.0	CVE-2008-3522 BID MISC MISC
kasseler-cms -- kasseler_cms	Multiple SQL injection vulnerabilities in Kasseler CMS 1.1.0 and 1.2.0 allow remote attackers to execute arbitrary SQL commands via (1) the nid parameter to index.php in a View action to the News module; (2) the vid parameter to index.php in a Result action to the Voting module; (3) the fid parameter to index.php in a ShowForum action to the Forum module; (4) the tid parameter to index.php in a ShowTopic action to the Forum module; (5) the uname parameter to index.php in a UserInfo action to the Account module; or (6) the module parameter to index.php, probably related to the TopSites module.	2008-09-30	7.5	CVE-2008-4356 BID MILW0RM
lansuite -- lansuite	Directory traversal vulnerability in index.php in LanSuite 3.3.2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the design parameter.	2008-09-30	7.5	CVE-2008-4330 BID MILW0RM
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	CVE-2008-4405 CONFIRM MISC CONFIRM MLIST MLIST MLIST
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	CVE-2008-4359 CONFIRM
lighttpd -- lighttpd	mod_userdir in lighttpd before 1.4.20, when a case-insensitive operating system or filesystem is used, performs case-sensitive 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.	2008-10-03	7.8	CVE-2008-4360 CONFIRM CONFIRM CONFIRM

linkarity -- linkarity	SQL injection vulnerability in link.php in Linkarity allows remote attackers to execute arbitrary SQL commands via the cat_id parameter. NOTE: although one component of Linkarity is distributable PHP code, this issue might be site-specific. If so, it should not be included in CVE.	2008-09-30	7.5	CVE-2008-4353 XF MILW0RM
livetvscript -- live_tv_script	SQL injection vulnerability in index.php in Live TV Script allows remote attackers to execute arbitrary SQL commands via the mid parameter.	2008-10-01	7.5	CVE-2008-4376 XF BID MILW0RM
microsoft -- iis	A certain ActiveX control in iisext.dll in Microsoft Internet Information Services (IIS) allows remote attackers to set a password via a string argument to the SetPassword method.	2008-09-29	10.0	CVE-2008-4301 BUGTRAQ
mozilla -- firefox	The user interface event dispatcher in Mozilla Firefox 3.0.3 on Windows XP SP2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a series of keypress, click, onkeydown, onkeyup, onmousedown, and onmouseup events. NOTE: it was later reported that Firefox 3.0.2 on Mac OS X 10.5 is also affected.	2008-09-29	7.5	CVE-2008-4324 BID BUGTRAQ BUGTRAQ MISC MISC MILW0RM MISC
mplayer -- mplayer	Multiple integer underflows in MPlayer 1.0_rc2 and earlier allow remote attackers to cause a denial of service (process termination) and possibly execute arbitrary code via a crafted video file that causes the stream_read function to read or write arbitrary memory.	2008-09-29	9.3	CVE-2008-3827 MISC
mr._cgi_guy -- hot_links_sql_php	SQL injection vulnerability in report.php in Mr. CGI Guy Hot Links SQL-PHP 3.0 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-01	7.5	CVE-2008-4378 BID MILW0RM
myblog -- myblog	add.php in MyBlog 0.9.8 and earlier allows remote attackers to bypass authentication and gain administrative access by setting a cookie with admin=yes and login=admin.	2008-09-30	7.5	CVE-2008-4341 BID MILW0RM FRSIRT
net_art_media -- iboutique	SQL injection vulnerability in the products module in NetArt Media iBoutique 4.0 allows remote attackers to execute arbitrary SQL commands via the cat parameter to index.php.	2008-09-30	7.5	CVE-2008-4354 BID MILW0RM FRSIRT
openengine -- openengine	PHP remote file inclusion vulnerability in cms/system/openengine.php in openEngine 2.0 beta4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the oe_classpath parameter.	2008-09-30	10.0	CVE-2008-4329 BID MILW0RM
outshine -- phportfolio	SQL injection vulnerability in photo.php in PHPortfolio allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-09-30	7.5	CVE-2008-4348 XF MISC
parsagostar -- parsaweb_cms	SQL injection vulnerability in default.aspx in ParsaGostar ParsaWeb CMS allows remote attackers to execute arbitrary SQL commands via the (1) id parameter in the "page" page and (2) txtSearch parameter in the "Search" page.	2008-09-30	7.5	CVE-2008-4364 XF BID BUGTRAQ MILW0RM

				MISC
phpocs -- phpocs	Directory traversal vulnerability in library/pagefunctions.inc.php in phpOCS 0.1 beta3 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the act parameter to index.php.	2008-09-30	7.5	CVE-2008-4331 BID MILW0RM
phpsmartcom -- phpsmartcom	Directory traversal vulnerability in index.php in phpSmartCom 0.2 allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the p parameter.	2008-09-30	7.5	CVE-2008-4351 BID MILW0RM
phpsmartcom -- phpsmartcom	SQL injection vulnerability in inc/pages/viewprofile.php in phpSmartCom 0.2 allows remote attackers to execute arbitrary SQL commands via the uid parameter in a viewprofile action to index.php.	2008-09-30	7.5	CVE-2008-4352 BID MILW0RM
powerportal -- powerportal	Directory traversal vulnerability in PowerPortal 2.0.13 allows remote attackers to list and possibly read arbitrary files via a .. (dot dot) in the path parameter to the default URI.	2008-09-30	7.8	CVE-2008-4361 XF BID MILW0RM
powie -- pnews	SQL injection vulnerability in newskom.php in Powie pNews 2.03 allows remote attackers to execute arbitrary SQL commands via the newsid parameter.	2008-09-30	7.5	CVE-2008-4347 BID MILW0RM
powie -- pforum	SQL injection vulnerability in showprofil.php in Powie PSCRIPT Forum (aka PHP Forum or pForum) 1.30 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-09-30	7.5	CVE-2008-4355 XF BID MILW0RM FRSIRT SECUNIA
powie -- plink	SQL injection vulnerability in linkto.php in Powie pLink 2.07 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-09-30	7.5	CVE-2008-4357 BID MILW0RM
project-observer -- observer	Observer 0.3.2.1 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in the query parameter to (1) whois.php or (2) netcmd.php.	2008-09-29	10.0	CVE-2008-4318 XF MILW0RM
realflex_technologies_ltd -- realwin_server	Stack-based buffer overflow in RealFlex Technologies Ltd. RealWin Server 2.0, as distributed by DATAC, allows remote attackers to execute arbitrary code via a crafted FC_INFOTAG/SET_CONTROL packet.	2008-09-29	10.0	CVE-2008-4322 XF BID BUGTRAQ SECUNIA MISC
redhat -- cman	The pserver_shutdown function in fence_egenera in cman 2.20080629 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/eglog temporary file.	2008-09-29	7.2	CVE-2008-4192 CONFIRM MLIST MLIST CONFIRM
ruby_on_rails -- ruby_on_rails	Multiple SQL injection vulnerabilities in Ruby on Rails before 2.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) :limit and (2) :offset parameters, related to ActiveRecord, ActiveSupport, ActiveResource, ActionPack, and ActionMailer.	2008-09-30	7.5	CVE-2008-4094 CONFIRM CONFIRM

safer_networking -- filealyzer	Stack-based buffer overflow in Safer Networking FileAlyzer 1.6.0.0 and 1.6.0.4 beta, and possibly other versions, allows user-assisted remote attackers to execute arbitrary code via an executable with malformed version data.	2008-10-02	9.3	CVE-2008-4396 XF BID MISC MISC MISC
samsung -- dvr_shr2040	The web interface in Samsung DVR SHR2040 allows remote attackers to cause a denial of service (crash) via a malformed HTTP request, related to the filter for configuration properties and "/x" characters.	2008-10-01	7.8	CVE-2008-4380 MISC BID MILW0RM SECUNIA
spaw_editor -- spaw_php	Unspecified vulnerability in class/theme.class.php in SPAW Editor PHP Edition before 2.0.8.1 has unknown impact and attack vectors, probably related to directory traversal sequences in the theme name.	2008-09-30	10.0	CVE-2008-4358 CONFIRM CONFIRM
talkback -- talkback	Directory traversal vulnerability in TalkBack 2.3.6 and 2.3.6.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the language parameter to comments.php, a different vector than CVE-2008-3371.	2008-09-30	7.5	CVE-2008-4346 BID MILW0RM SECUNIA
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	CVE-2008-4402 BID
vblogix -- tutorial_script	SQL injection vulnerability in main.php in vbLOGIX Tutorial Script 1.0 and earlier allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a list action.	2008-09-30	7.5	CVE-2008-4350 BID MILW0RM FRSIRT
webportal -- webportal_cms	SQL injection vulnerability in download.php in WebPortal CMS 0.7.4 and earlier allows remote attackers to execute arbitrary SQL commands via the aid parameter.	2008-09-30	7.5	CVE-2008-4345 BID MILW0RM FRSIRT

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
apple -- mac_os_x	The default configuration of Java 1.5 on Apple Mac OS X 10.5.4 and 10.5.5 contains a jurisdiction policy that limits Java Cryptography Extension (JCE) key sizes to 128 bits, which makes it easier for attackers to decrypt ciphertext produced by JCE.	2008-10-01	5.0	CVE-2008-4368 CONFIRM APPLE
atomic_photo_album -- atomic_photo_album	Cross-site scripting (XSS) vulnerability in album.php in Atomic Photo Album (APA) 1.1.0pre4 allows remote attackers to inject arbitrary web	2008-09-30	4.3	CVE-2008-4336 BID MILW0RM

	script or HTML via the apa_album_ID parameter.			
availscript -- availscript_photo_album	Multiple cross-site scripting (XSS) vulnerabilities in Availscript Photo Album allow remote attackers to inject arbitrary web script or HTML via the (1) sid parameter to pics.php and the (2) a parameter to view.php.	2008-10-01	4.3	CVE-2008-4370 BID MILW0RM
availscript -- availscript_article_script	Cross-site scripting (XSS) vulnerability in articles.php in AvailScript Article Script allows remote attackers to inject arbitrary web script or HTML via the aIDS parameter.	2008-10-01	4.3	CVE-2008-4372 BID MILW0RM
bitweaver -- bitweaver	Cross-site scripting (XSS) vulnerability in Bitweaver 2.0.2 allows remote attackers to inject arbitrary web script or HTML via the URL parameter to (1) edit.php and (2) list.php in articles/; (3) list_blogs.php and (4) rankings.php in blogs/; (5) calendar/index.php; (6) calendar.php, (7) index.php, and (8) list_events.php in events/; (9) index.php and (10) list_galleries.php in fisheye/; (11) liberty/list_content.php; (12) newsletters/edition.php; (13) pigeonholes/list.php; (14) recommends/index.php; (15) rss/index.php; (16) stars/index.php; (17) users/remind_password.php; (18) wiki/orphan_pages.php; and (19) stats/index.php, different vectors than CVE-2007-0526 and CVE-2005-4379. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-30	4.3	CVE-2008-4337 XF BID SECUNIA
blosxom -- blosxom	Cross-site scripting (XSS) vulnerability in blosxom.cgi in Blosxom before 2.1.2 allows remote attackers to inject arbitrary web script or HTML via the flav parameter (flavour variable). NOTE: some of these details are obtained from third party information.	2008-10-03	4.3	CVE-2008-2236 CONFIRM SECUNIA

camera_life -- camera_life	Unrestricted file upload vulnerability in the image upload component in Camera Life 2.6.2b4 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in a user directory under images/photos/upload.	2008-09-30	6.5	CVE-2008-4366 XF BID MILW0RM
cannot -- php_infoboard	Cross-site scripting (XSS) vulnerability in PHP infoBoard V.7 Plus allows remote attackers to inject arbitrary web script or HTML via the idcat parameter in a newtopic action.	2008-09-30	4.3	CVE-2008-4333 BID MILW0RM
cisco -- ios	A "logic error" in Cisco IOS 12.0 through 12.4, when a Multiprotocol Label Switching (MPLS) VPN with extended communities is configured, sometimes causes a corrupted route target (RT) to be used, which allows remote attackers to read traffic from other VPNs in opportunistic circumstances.	2008-09-26	5.1	CVE-2008-3803 CISCO
deslock -- deslock	The Virtual Token driver (vdlptokn.sys) 1.0.2.43 in DESlock+ 3.2.7 allows local users to cause a denial of service (system crash) via a crafted IOCTL request to \Device\DLPTokenWalter0.	2008-09-30	4.9	CVE-2008-4362 MILW0RM FRSIRT SECUNIA
flatpress -- flatpress	Multiple cross-site scripting (XSS) vulnerabilities in FlatPress 0.804 allow remote attackers to inject arbitrary web script or HTML via the (1) user or (2) pass parameter to login.php, or the (3) name parameter to contact.php.	2008-09-29	4.3	CVE-2008-4120 BUGTRAQ CONFIRM MISC
google -- chrome	Google Chrome 0.2.149.29 and 0.2.149.30 allows remote attackers to cause a denial of service (memory consumption) via an HTML document containing a carriage return ("\r\n\r\n") argument to the window.open function.	2008-09-30	4.3	CVE-2008-4340 BID BUGTRAQ MILW0RM MISC
kde -- konqueror	Konqueror in KDE 3.5.9 allows remote attackers to cause a denial of service (application crash) via Javascript that calls the alert function with a URL-encoded string of a large	2008-10-02	5.0	CVE-2008-4382 BUGTRAQ

	number of invalid characters.			
libra_file_manager -- php_filemanager	fileadmin.php in Libra File Manager (aka Libra PHP File Manager) 1.18 and earlier allows remote attackers to bypass authentication, and read arbitrary files, modify arbitrary files, and list arbitrary directories, by inserting certain user and isadmin parameters in the query string.	2008-09-29	6.4	CVE-2008-4319 BID BUGTRAQ MILW0RM
lighttpd -- lighttpd	Memory leak in the http_request_parse function in request.c in lighttpd before 1.4.20 allows remote attackers to cause a denial of service (memory consumption) via a large number of requests with duplicate request headers.	2008-09-27	5.0	CVE-2008-4298 CONFIRM
linux -- kernel	fs/open.c in the Linux kernel before 2.6.22 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 creating an executable file in a setgid directory through the (1) truncate or (2) ftruncate function in conjunction with memory-mapped I/O.	2008-09-29	4.6	CVE-2008-4210 CONFIRM BID MLIST MLIST CONFIRM CONFIRM CONFIRM
linux -- kernel	fs/splice.c in the splice subsystem in the Linux kernel before 2.6.22.2 does not properly handle a failure of the add_to_page_cache_lru function, and subsequently attempts to unlock a page that was not locked, which allows local users to cause a denial of service (kernel BUG and system crash), as demonstrated by the fio I/O tool.	2008-09-29	4.9	CVE-2008-4302 CONFIRM XF BID MLIST MISC MLIST CONFIRM CONFIRM
linux -- kernel redhat -- fedora	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	2008-10-03	4.9	CVE-2008-3833 CONFIRM MLIST CONFIRM

	inode in order to create an executable file in a setgid directory, a different vulnerability than CVE-2008-4210.			
microsoft -- internet_authentication_service_helper_com_component	A certain ActiveX control in the Microsoft Internet Authentication Service (IAS) Helper COM Component in iashlpr.dll allows remote attackers to cause a denial of service (browser crash) via a large integer value in the first argument to the PutProperty method.	2008-09-29	5.0	CVE-2008-4299 BUGTRAQ
microsoft -- iis	A certain ActiveX control in adsiis.dll in Microsoft Internet Information Services (IIS) allows remote attackers to cause a denial of service (browser crash) via a long string in the second argument to the GetObject method.	2008-09-29	5.0	CVE-2008-4300 BUGTRAQ
microsoft -- windows_xp	Windows Explorer in Microsoft Windows XP SP3 allows user-assisted attackers to cause a denial of service (application crash) via a crafted .ZIP file.	2008-09-29	4.3	CVE-2008-4323 MILW0RM
microsoft -- windows_xp	gdiplus.dll in GDI+ in Microsoft Windows XP SP3 does not properly handle crafted .ico files, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a certain crash.ico file on a web site, and allows user-assisted attackers to cause a denial of service (divide-by-zero error and persistent application crash) via this crash.ico file on the desktop, a different vulnerability than CVE-2007-2237.	2008-09-30	4.3	CVE-2008-4327 BID MILW0RM
microsoft -- internet_explorer	Microsoft Internet Explorer 7 allows remote attackers to cause a denial of service (application crash) via Javascript that calls the alert function with a URL-encoded string of a large number of invalid characters.	2008-10-02	5.0	CVE-2008-4381 BUGTRAQ
mr._cgi_guy -- hot_links_sql_php	Cross-site scripting (XSS) vulnerability in report.php in	2008-10-01	4.3	CVE-2008-4379 MILW0RM

	Mr. CGI Guy Hot Links SQL-PHP 3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the id parameter.			
opennms.org -- opennms	Multiple cross-site scripting (XSS) vulnerabilities in OpenNMS before 1.5.94 allow remote attackers to inject arbitrary web script or HTML via (1) the j_username parameter to j_acegi_security_check, (2) the username parameter to notification/list.jsp, and (3) the filter parameter to event/list.	2008-09-29	4.3	CVE-2008-4320 BID CONFIRM
phpmyadmin -- phpmyadmin	The PMA_escapeJsString function in libraries/js_escape.lib.php in phpMyAdmin before 2.11.9.2, when Internet Explorer is used, allows remote attackers to bypass cross-site scripting (XSS) protection mechanisms and conduct XSS attacks via a NUL byte inside a "	2008-09-30	4.3	CVE-2008-4326 CONFIRM CONFIRM MLIST CONFIRM CONFIRM
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 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.	2008-10-03	4.4	CVE-2008-3825 CONFIRM REDHAT
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 BID MLIST MISC
s0nic -- paranews	Multiple cross-site scripting (XSS) vulnerabilities in news.php in s0nic Paranews 3.4 allow remote attackers to inject arbitrary web script or HTML	2008-09-30	4.3	CVE-2008-4349 BID SECUNIA MISC

	via the (1) id or (2) page parameter in a details action.			
siteman -- siteman	Cross-site scripting (XSS) vulnerability in search.php in Siteman 1.1.11 and earlier allows remote attackers to inject arbitrary web script or HTML via unknown vectors. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-09-30	4.3	CVE-2008-4365 XF BID
symantec -- netbackup_enterprise_server symantec -- netbackup_server	Unspecified vulnerability in the Java Administration GUI (jnbSA) in Symantec Veritas NetBackup Server and NetBackup Enterprise Server 5.1 before MP7, 6.0 before MP7, and 6.5 before 6.5.2 allows remote authenticated users to gain privileges via unknown attack vectors related to "bpjava* binaries."	2008-09-30	6.5	CVE-2008-4339 CONFIRM
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 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.	2008-10-03	5.0	CVE-2008-2439 CONFIRM CONFIRM CONFIRM CONFIRM FRSIRT SECUNIA SECUNIA
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 BID FRSIRT SECUNIA
vacilanda -- brilliant_gallery	SQL injection vulnerability in the brilliant_gallery_checklist_save function in the bgchecklist/save	2008-09-30	6.0	CVE-2008-4338 XF BID BUGTRAQ

	script in Brilliant Gallery 5.x and 6.x, a module for Drupal, allows remote authenticated users with "access brilliant_gallery" permissions to execute arbitrary SQL commands via the (1) nid, (2) qid, (3) state, and possibly (4) user parameters.			SECUNIA FULLDISC CONFIRM
viewvc -- viewvc	lib/viewvc.py in ViewVC 1.0.5 uses the content-type parameter in the HTTP request for the Content-Type header in the HTTP response, which allows remote attackers to cause content to be misinterpreted by the browser via a content-type parameter that is inconsistent with the requested object. NOTE: this issue might not be a vulnerability, since it requires attacker access to the repository that is being viewed.	2008-09-30	5.8	CVE-2008-4325 CONFIRM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
mailmarshal -- e10000_appliance mailmarshal -- smtp	Multiple cross-site scripting (XSS) vulnerabilities in the delegated spam management feature in the Spam Quarantine Management (SQM) component in MailMarshal SMTP 6.0.3.8 through 6.3.0.0 allow user-assisted remote authenticated users to inject arbitrary web script or HTML via (1) the list of blocked senders or (2) the list of safe senders.	2008-10-02	3.5	CVE-2008-2831 XF XF BID CONFIRM MISC SECUNIA

Back to top