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

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

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

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

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
1scripts -- z1exchange	SQL injection vulnerability in showads.php in Z1Exchange allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-03-02	7.5	CVE-2008-6392 XF MISC
3com -- wireless_8760_dual-radio	The web management interface in 3Com Wireless 8760 Dual Radio 11a/b/g PoE Access Point allows remote attackers to cause a denial of service (device crash) via a malformed HTTP POST request.	2009-03-04	7.8	CVE-2008-6395 XF BID SECUNIA FULLDISC
activewebsoftwares -- active_web_helpdesk	SQL injection vulnerability in default.aspx in Active Web Helpdesk 2.0 allows remote attackers to execute arbitrary SQL commands via the CategoryID parameter.	2009-03-02	7.5	CVE-2008-6380 XF BID MILW0RM SECUNIA
adserversolutions --	SQL injection vulnerability in logon_process.jsp in Ad Server Solutions Banner Exchange Solution Java allows remote attackers to execute arbitrary SQL	2009-03-	7.5	CVE-2008-6364 XF BID

banner_exchange_software	commands via the (1) username (uname parameter) and (2) password (pass parameter). NOTE: some of these details are obtained from third party information.	02	7.5	BID MILW0RM SECUNIA MISC
adserversolutions -- ad_management_software	SQL injection vulnerability in logon.jsp in Ad Server Solutions Ad Management Software Java allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password, related to the uname or pass parameters to logon.jsp or logon_processing.jsp. NOTE: some of these details are obtained from third party information.	2009-03-02	7.5	CVE-2008-6365 XF BID MILW0RM SECUNIA
adserversolutions -- affiliate_software_java	SQL injection vulnerability in logon.jsp in Ad Server Solutions Affiliate Software Java 4.0 allows remote attackers to execute arbitrary SQL commands via the (1) username and (2) password, possibly related to the uname and pass parameters to logon_process.jsp. NOTE: some of these details are obtained from third party information.	2009-03-02	7.5	CVE-2008-6366 XF BID MILW0RM SECUNIA MISC
aj_square -- aj_auction	SQL injection vulnerability in detail.php in AJ Auction Pro Platinum Skin 2 allows remote attackers to execute arbitrary SQL commands via the item_id parameter.	2009-03-06	7.5	CVE-2008-6414 MILW0RM
aliensoftcorp -- rae_media_contact_management	SQL injection vulnerability in asadmin/default.asp in Rae Media Contact Management Software SOHO, Standard, and Enterprise allows remote attackers to execute arbitrary SQL commands via the Password parameter. NOTE: some of these details are obtained from third party information.	2009-03-02	7.5	CVE-2008-6389 BID MILW0RM SECUNIA
andrew_freed -- quotebook	Multiple SQL injection vulnerabilities in QuoteBook allow remote attackers to execute arbitrary SQL commands via the (1) MyBox and (2) selectFavorites parameters to (a) quotes.php and the (3) QuoteName and (4) QuoteText parameters to (b) quotesadd.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-05	7.5	CVE-2009-0829 SECUNIA
ausimods -- e-cart	SQL injection vulnerability in items.php in the E-Cart module 1.3 for PHP-Fusion allows remote attackers to execute arbitrary SQL commands via the CA parameter	2009-03-05	7.5	CVE-2009-0832 BID BUGTRAQ

	SQL commands via the CA parameter.			MILW0RM
avahi -- avahi-daemon	The originates_from_local_legacy_unicast_socket function in avahi-core/server.c in avahi-daemon 0.6.23 does not account for the network byte order of a port number when processing incoming multicast packets, which allows remote attackers to cause a denial of service (network bandwidth and CPU consumption) via a crafted legacy unicast mDNS query packet that triggers a multicast packet storm.	2009-03-03	7.8	CVE-2009-0758 MLIST MISC
bookelves -- kipper	Directory traversal vulnerability in index.php in Kipper 2.01 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the configfile parameter.	2009-03-06	7.5	CVE-2009-0765 BID MILW0RM SECUNIA
bookelves -- kipper	Directory traversal vulnerability in default.php in Kipper 2.01 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the configfile parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-06	7.5	CVE-2009-0766 SECUNIA
bpsoft -- hex_workshop	Stack-based buffer overflow in BreakPoint Software Hex Workshop 4.23, 6.0.1.4603, and other 6.x and earlier versions allows remote attackers to execute arbitrary code via a crafted Intel Hex Code (.hex) file. NOTE: some of these details are obtained from third party information.	2009-03-04	9.3	CVE-2009-0812 XF BID BUGTRAQ MILW0RM SECUNIA
brian_wilson -- ol'bookmarks	Directory traversal vulnerability in frame.php in ol'bookmarks manager 0.7.5 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the framefile parameter.	2009-03-06	7.5	CVE-2008-6407 BID MILW0RM
brian_wilson -- ol'bookmarks	PHP remote file inclusion vulnerability in frame.php in ol'bookmarks manager 0.7.5 allows remote attackers to execute arbitrary PHP code via a URL in the framefile parameter.	2009-03-06	7.5	CVE-2008-6408 BID MILW0RM
brian_wilson -- ol'bookmarks	SQL injection vulnerability in index.php in ol'bookmarks manager 0.7.5 allows remote attackers to execute arbitrary SQL commands via the id parameter in a brain	2009-03-06	7.5	CVE-2008-6409 MILW0RM

	action.			
brian_wilson -- ol'bookmarks	Directory traversal vulnerability in show.php in ol'bookmarks manager 0.7.5 and earlier allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the show parameter.	2009-03-06	7.5	CVE-2008-6410 BID MILW0RM
capilano -- designworks	Stack-based buffer overflow in DesignWorks Professional 4.3.1 and 5.0.7 allows remote attackers to execute arbitrary code via a crafted .cct file. NOTE: some of these details are obtained from third party information.	2009-03-02	9.3	CVE-2008-6363 VUPEN BID MILW0RM SECUNIA
chipmunk_scripts -- chipmunk_guestbook	SQL injection vulnerability in index.php in Chipmunk Guestbook 1.4m allows remote attackers to execute arbitrary SQL commands via the start parameter.	2009-03-02	7.5	CVE-2008-6368 XF SECUNIA MISC OSVDB
cisco -- session_border_controller	Unspecified vulnerability in the Session Border Controller (SBC) before 3.0(2) for Cisco 7600 series routers allows remote attackers to cause a denial of service (SBC card reload) via crafted packets to TCP port 2000.	2009-03-04	7.8	CVE-2009-0619 XF BID CISCO
cosmin_truta -- optipng	Use-after-free vulnerability in the GIFReadNextExtension function in lib/pngxtern/gif/gifread.c in OptiPNG 0.6.2 and earlier allows context-dependent attackers to cause a denial of service (application crash) via a crafted GIF image that causes the realloc function to return a new pointer, which triggers memory corruption when the old pointer is accessed.	2009-03-02	9.3	CVE-2009-0749 VUPEN BID CONFIRM
cs-cart -- cs-cart	SQL injection vulnerability in core/user.php in CS-Cart 1.3.5 and earlier allows remote attackers to execute arbitrary SQL commands via the cs_cookies[customer_user_id] cookie parameter.	2009-03-04	7.5	CVE-2008-6394 XF BID BUGTRAQ MILW0RM MISC SECUNIA
explay -- explay_cms	Explay CMS 2.1 and earlier allows remote attackers to bypass authentication and gain administrative access by setting the login cookie to 1.	2009-03-06	7.5	CVE-2008-6411 XF BID MILW0RM

ezonelink -- multiple_membership_script	SQL injection vulnerability in sitepage.php in Multiple Membership Script 2.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-03-02	7.5	CVE-2008-6362 BID MILW0RM SECUNIA
greatclone -- hotscripts_clone	SQL injection vulnerability in showcategory.php in Hotscripts Clone allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-03-06	7.5	CVE-2008-6405 BID MILW0RM
ibm -- aix	Buffer overflow in pppdial in IBM AIX 5.3 and 6.1 allows local users to gain privileges via a long "input string."	2009-03-04	7.2	CVE-2009-0779 VUPEN AIXAPAR AIXAPAR AIXAPAR AIXAPAR
imera -- teamlinks	Insecure method vulnerability in the ImeraIEPlugin ActiveX control (ImeraIEPlugin.dll 1.0.2.54) in Imera TeamLinks Client allows remote attackers to force the download and execution of arbitrary URLs via modified DownloadProtocol, DownloadHost, DownloadPort, and DownloadURI parameters.	2009-03-04	9.3	CVE-2009-0813 XF VUPEN MILW0RM SECUNIA
jetik -- jetik-web	SQL injection vulnerability in sayfa.php in JETIK-WEB allows remote attackers to execute arbitrary SQL commands via the kat parameter.	2009-03-06	7.5	CVE-2008-6401 BID MILW0RM
linux -- kernel	The audit_syscall_entry function in the Linux kernel 2.6.28.7 and earlier on the x86_64 platform does not properly handle (1) a 32-bit process making a 64-bit syscall or (2) a 64-bit process making a 32-bit syscall, which allows local users to bypass certain syscall audit configurations via crafted syscalls, a related issue to CVE-2009-0342 and CVE-2009-0343.	2009-03-06	7.2	CVE-2009-0834 CONFIRM XF BID SECUNIA MISC MLIST MLIST MLIST CONFIRM
linux -- kernel	The __secure_computing function in kernel/seccomp.c in the seccomp subsystem in the Linux kernel 2.6.28.7 and earlier on the x86_64 platform, when CONFIG_SECCOMP is enabled, does not properly handle (1) a 32-bit process making	2009-03-	7.2	CVE-2009-0835 MISC SECUNIA MISC

linux -- kernel	a 64-bit syscall or (2) a 64-bit process making a 32-bit syscall, which allows local users to bypass intended access restrictions via crafted syscalls that are misinterpreted as (a) stat or (b) chmod, a related issue to CVE-2009-0342 and CVE-2009-0343.	06	7.2	MISC MISC MLIST MLIST MLIST
manzovi -- proquiz	SQL injection vulnerability in index.php in ProQuiz 1.0 allows remote attackers to execute arbitrary SQL commands via the password parameter, a different vector than CVE-2008-6312.	2009-02-27	7.5	CVE-2008-6327 XF XF MILW0RM
mega-nerd -- libsndfile nullsoft -- winamp	Integer overflow in libsndfile 1.0.18, as used in Winamp and other products, allows context-dependent attackers to execute arbitrary code via crafted description chunks in a CAF audio file, leading to a heap-based buffer overflow.	2009-03-04	9.3	CVE-2009-0186 VUPEN VUPEN BID BUGTRAQ BUGTRAQ CONFIRM MISC MISC SECUNIA SECUNIA
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via certain vectors that trigger memory corruption and assertion failures.	2009-03-04	10.0	CVE-2009-0771 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to nsCSSStyleSheet::GetOwnerNode, events, and garbage collection, which triggers memory corruption.	2009-03-04	9.3	CVE-2009-0772 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey	The JavaScript engine in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via (1) a splice of an array that contains "some non-set elements," which causes jsarray.cpp to pass an incorrect argument to the ResizeSlots	2009-03-	10.0	CVE-2009-0773

mozilla -- seamonkey mozilla -- thunderbird	function, which triggers memory corruption; (2) vectors related to js_DecompileValueGenerator, jsopcode.cpp, __defineSetter__, and watch, which triggers an assertion failure or a segmentation fault; and (3) vectors related to gczeal, __defineSetter__, and watch, which triggers a hang.	04	10.0	0773 CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 2 and 3 before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey 1.1.15 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to gczeal, a different vulnerability than CVE-2009-0773.	2009-03-04	9.3	CVE-2009-0774 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Double free vulnerability in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to execute arbitrary code via "cloned XUL DOM elements which were linked as a parent and child," which are not properly handled during garbage collection.	2009-03-04	10.0	CVE-2009-0775 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	nsIRDFService in Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 allows remote attackers to bypass the same-origin policy and read XML data from another domain via a cross-domain redirect.	2009-03-04	7.1	CVE-2009-0776 CONFIRM CONFIRM
mpfr -- gnu_mpfr	Multiple buffer overflows in GNU MPFR 2.4.0 allow context-dependent attackers to cause a denial of service (crash) via the (1) mpfr_snprintf and (2) mpfr_vsnprintf functions.	2009-03-03	7.5	CVE-2009-0757 MLIST CONFIRM
muskatli -- sofi_webgui	PHP remote file inclusion vulnerability in hu/modules/reg-new/modstart.php in Sofi WebGui 0.6.3 PRE and earlier allows remote attackers to execute arbitrary PHP code via a URL in the mod_dir parameter.	2009-03-06	7.5	CVE-2008-6402 BID MILW0RM
mxmania -- calendar_mx_professional	SQL injection vulnerability in calendar_Eventupdate.asp in Calendar Mx Professional 2.0.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2009-03-02	7.5	CVE-2008-6378 XF BID MILW0RM SECUNIA
	SQL injection vulnerability in pics_pre.asp			CVE-2008-6379

mxmania -- gallery_mx	in Gallery MX 2.0.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter.	2009-03-02	7.5	XF BID MILW0RM SECUNIA
myplugins -- gen_msn	Heap-based buffer overflow in gen_msn.dll in the gen_msn plugin 0.31 for Winamp 5.541 allows remote attackers to execute arbitrary code via a playlist (.pls) file with a long URL in the File1 field. NOTE: some of these details are obtained from third party information.	2009-03-05	9.3	CVE-2009-0833 BID MILW0RM SECUNIA
nexusjnr -- jbook	SQL injection vulnerability in main.asp in Jbook allows remote attackers to execute arbitrary SQL commands via the password (pass parameter).	2009-03-02	7.5	CVE-2008-6376 XF BID MISC
nexusjnr -- jbook	SQL injection vulnerability in main.asp in Jbook allows remote attackers to execute arbitrary SQL commands via the username (user parameter).	2009-03-02	7.5	CVE-2008-6391 XF
ocean12tech -- contact_manager_pro	SQL injection vulnerability in default.asp in Ocean12 Contact Manager Pro 1.02 allows remote attackers to execute arbitrary SQL commands via the Sort parameter.	2009-03-02	7.5	CVE-2008-6369 XF BID MILW0RM SECUNIA OSVDB
ocean12tech -- membership_manager_pro	SQL injection vulnerability in login.asp in Ocean12 Membership Manager Pro allows remote attackers to execute arbitrary SQL commands via the username (Username parameter).	2009-03-02	7.5	CVE-2008-6371 XF BID MILW0RM SECUNIA OSVDB
ocean12tech -- faq_manager_pro	SQL injection vulnerability in default.asp in Ocean12 FAQ Manager Pro 1.0 allows remote attackers to execute arbitrary SQL commands via the ID parameter in a Cat action. NOTE: some of these details are obtained from third party information.	2009-03-02	7.5	CVE-2008-6372 BID MILW0RM SECUNIA
ocean12tech -- membership_manager_pro	SQL injection vulnerability in login.asp in Ocean12 Membership Manager Pro allows remote attackers to execute arbitrary SQL commands via the Password parameter. NOTE: the provenance of this information is unknown; the details are obtained solely	2009-03-02	7.5	CVE-2008-6390 XF OSVDB MILW0RM SECUNIA

	from third party information.			SECUNIA
openrat -- openrat	PHP remote file inclusion vulnerability in themes/default/include/html/insert.inc.php in OpenRat 0.8-beta4 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the tpl_dir parameter.	2009-03-06	7.5	CVE-2008-6403 BID MILW0RM
php.brickhost -- phpscheduleit	Multiple eval injection vulnerabilities in phpScheduleIt before 1.2.11 allow remote attackers to execute arbitrary code via (1) the end_date parameter to reserve.php and (2) the start_date and end_date parameters to check.php. NOTE: the start_date/reserve.php vector is already covered by CVE-2008-6132.	2009-03-04	7.5	CVE-2009-0820 VUPEN CONFIRM CONFIRM CONFIRM
phpbb-seo -- multi_seo_phpbb	PHP remote file inclusion vulnerability in include/global.php in Multi SEO phpBB 1.1.0 allows remote attackers to execute arbitrary PHP code via a URL in the pfad parameter.	2009-03-02	7.5	CVE-2008-6377 BID MILW0RM SECUNIA
psi-im -- psi	PSI Jabber client before 0.12.1 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a file transfer request with a negative value in a SOCKS5 option, which bypasses a signed integer check and triggers an integer overflow and a heap-based buffer overflow.	2009-03-03	10.0	CVE-2008-6393 CONFIRM
qbik -- wingate	Qbik WinGate, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.	2009-03-04	7.1	CVE-2009-0802 CERT-VN BID
simple_cmms -- simplecmms	Multiple SQL injection vulnerabilities in SimpleCMMS before 0.1.0 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	2009-03-04	7.5	CVE-2009-0808 XF VUPEN CONFIRM
sixapart -- movable_type	Unspecified vulnerability in Movable Type Pro and Community Solution 4.x before 4.24 has unknown impact and attack vectors, possibly related to the password recovery mechanism.	2009-03-02	10.0	CVE-2009-0752 CONFIRM

smoothwall -- networkguardian smoothwall -- schoolguardian smoothwall -- smoothguardian	SmoothWall SmoothGuardian, as used in SmoothWall Firewall, NetworkGuardian, and SchoolGuardian 2008, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.	2009-03-04	7.1	CVE-2009-0803 CERT-VN BID CONFIRM
socialgroupie -- social_groupie	SQL injection vulnerability in group_index.php in Social Groupie allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-03-02	7.5	CVE-2008-6358 BID MILW0RM SECUNIA
socialgroupie -- social_groupie	Unrestricted file upload vulnerability in Photos/create_album.php in Social Groupie 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 Member_images/.	2009-03-02	8.5	CVE-2008-6367 MILW0RM SECUNIA
sopcast -- sopcore_activex_control	Insecure method vulnerability in the SopCast SopCore ActiveX control in sopocx.ocx 3.0.3.501 allows remote attackers to execute arbitrary programs via an executable file name in the argument to the SetExternalPlayer method.	2009-03-04	7.5	CVE-2009-0811 XF BID BUGTRAQ MISC
squid -- squid_web_proxy_cache	Squid, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.	2009-03-04	7.1	CVE-2009-0801 CERT-VN BID
tombstone -- smnews	SQL injection vulnerability in login.php in the smNews example script for txtSQL 2.2 Final allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-03-02	7.5	CVE-2009-0750 XF MILW0RM
torrenttrader -- torrenttrader	SQL injection vulnerability in scrape.php in TorrentTrader before 2008-05-13 allows	2009-03-	7.5	CVE-2008-6418

torrenttrader -- torrenttrader	remote attackers to execute arbitrary SQL commands via the info_hash parameter.	06	7.5	BID CONFIRM
vignette -- vignette_content_management	Unspecified vulnerability in Vignette Content Management 7.3.0.5, 7.3.1, 7.3.1.1, 7.4, and 7.5 allows "low privileged" users to gain administrator privileges via unknown attack vectors.	2009-03-06	7.5	CVE-2008-6412 CONFIRM
wesnoth -- wesnoth	The Python AI module in Wesnoth 1.4.x and 1.5 before 1.5.11 allows remote attackers to escape the sandbox and execute arbitrary code by using a whitelisted module that imports an unsafe module, then using a hierarchical module name to access the unsafe module through the whitelisted module.	2009-03-04	9.3	CVE-2009-0367 CONFIRM CONFIRM VUPEN
xatrix -- xguestbook	SQL injection vulnerability in login.php in xGuestbook 2.0 allows remote attackers to execute arbitrary SQL commands via the user parameter.	2009-03-04	7.5	CVE-2009-0810 XF VUPEN BID MILW0RM
yapbb -- yapbb	SQL injection vulnerability in forumhop.php in YapBB 1.2 and earlier allows remote attackers to execute arbitrary SQL commands via the forumID parameter in a next action.	2009-03-06	7.5	CVE-2009-0768 BID MILW0RM
youngzsoft -- ccproxy	Buffer overflow in YoungZSoft CCProxy 6.5 might allow remote attackers to execute arbitrary code via a CONNECTION request with a long hostname.	2009-03-06	10.0	CVE-2008-6415 XF SECTRACK SECUNIA MISC
zfeeder -- zfeeder	zFeeder 1.6 allows remote attackers to gain administrative access via a direct request to admin.php.	2009-03-04	7.5	CVE-2009-0807 XF MILW0RM
ziproxy -- ziproxy	Ziproxy 2.6.0, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.	2009-03-04	7.1	CVE-2009-0804 CERT-VN BID CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
1scripts -- z1exchange	Cross-site scripting (XSS) vulnerability in showads.php in Z1Exchange 1.0 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	2009-03-02	4.3	CVE-2008-6386 XF MISC
4u2ges -- rapid_classified	Rapid Classified 3.1 and 3.15 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request to cldb.mdb.	2009-03-02	5.0	CVE-2008-6388 XF MILW0RM
activewebsoftwares -- quick_tree_view_.net	Quick Tree View .NET 3.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request to qtv.mdb.	2009-03-02	5.0	CVE-2008-6387 VUPEN MILW0RM
andrew_freed -- pollhelper	PollHelper stores poll.inc under the web root with insufficient access control, which allows remote attackers to download the database file containing user credentials via a direct request.	2009-03-05	5.0	CVE-2009-0827 XF MILW0RM SECUNIA OSVDB
andrew_freed -- quotebook	Cross-site scripting (XSS) vulnerability in QuoteBook allows remote attackers to inject arbitrary web script or HTML via the (1) QuoteName and (2) QuoteText parameters to quotesadd.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-05	4.3	CVE-2009-0830 SECUNIA
aspportal -- aspportal	ASP Portal 3.2.5 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request to ASPPortal.mdb.	2009-03-02	5.0	CVE-2008-6382 MILW0RM SECUNIA OSVDB
bcoos -- bcoos	SQL injection vulnerability in modules/adresses/viewcat.php in bcoos 1.0.13, and possibly earlier, allows remote authenticated users with	2009-03-02	4.6	CVE-2008-6381 XF BID

	Addresses module permissions to execute arbitrary SQL commands via the cid parameter.	02		MILW0RM SECUNIA OSVDB
blogsa -- blogsa	Cross-site scripting (XSS) vulnerability in Widgets.aspx in Blogsa 1.0 Beta 3 and earlier allows remote attackers to inject arbitrary web script or HTML via the searchText parameter.	2009-03-04	4.3	CVE-2009-0814 XF BID BUGTRAQ
bookelves -- kipper	Cross-site scripting (XSS) vulnerability in default.php in Kipper 2.01 allows remote attackers to inject arbitrary web script or HTML via the charm parameter.	2009-03-06	4.3	CVE-2009-0763 BID MILW0RM SECUNIA
bookelves -- kipper	Multiple cross-site scripting (XSS) vulnerabilities in Kipper 2.01 allow remote attackers to inject arbitrary web script or HTML via the charm parameter to (1) index.php and (2) kipper.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-06	4.3	CVE-2009-0764 SECUNIA
bookelves -- kipper	Kipper 2.01 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a file containing credentials via a direct request for job/config.data.	2009-03-06	5.0	CVE-2009-0767 MILW0RM SECUNIA
celerondude -- uploader	Cross-site scripting (XSS) vulnerability in account.php in Celerondude Uploader 6.1 allows remote attackers to inject arbitrary web script or HTML via the username parameter. NOTE: some of these details are obtained from third party information.	2009-03-04	4.3	CVE-2008-6396 XF BID SECUNIA MISC
codefixer -- mailinglistpro	CodefixerSoftware MailingListPro Free Edition stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain sensitive information via a direct request to db/MailingList.mdb.	2009-03-02	5.0	CVE-2008-6374 XF MILW0RM SECUNIA
	The redirect implementation in curl and libcurl 5.11 through 7.19.3, when CURLOPT_FOLLOWLOCATION is enabled, accepts arbitrary Location			CVE-2009-0037

curl -- curl curl -- libcurl	values, which might allow remote HTTP servers to (1) trigger arbitrary requests to intranet servers, (2) read or overwrite arbitrary files via a redirect to a file: URL, or (3) execute arbitrary commands via a redirect to an scp: URL.	2009-03-04	6.8	VUPEN BID CONFIRM CONFIRM
datalifecms -- datalife_engine	Cross-site scripting (XSS) vulnerability in admin.php in DataLife Engine (DLE) 7.2 allows remote attackers to inject arbitrary web script or HTML via the query string.	2009-03-06	4.3	CVE-2008-6406 XF BID BUGTRAQ SECUNIA
dkim -- dkim-milter	dkim-milter 2.6.0 through 2.8.0 allows remote attackers to cause a denial of service (crash) by signing a message with a key that has been revoked in DNS, which triggers an assertion error.	2009-03-06	5.0	CVE-2009-0770 BID DEBIAN CONFIRM
donnafontenot -- evcal_events_calendar	evCal Events Calendar stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing the username and password via a direct request to (1) evcal.mdb and (2) evcal97.mdb.	2009-03-02	5.0	CVE-2008-6356 XF MILW0RM
donnafontenot -- mycal_personal_events_calendar	MyCal Personal Events Calendar stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing the username and password via a direct request to mycal.mdb.	2009-03-02	5.0	CVE-2008-6357 XF MILW0RM
dotnetnuke -- dotnetnuke	Unspecified vulnerability in DotNetNuke 4.5.2 through 4.9 allows remote attackers to "add additional roles to their user account" via unknown attack vectors.	2009-03-05	5.5	CVE-2008-6399 BID CONFIRM SECUNIA OSVDB
drupal -- storm	SQL injection vulnerability in SpeedTech Organization and Resource Manager (Storm) 5.x before 5.x-1.14 and 6.x before 6.x-1.18, a module for Drupal, allows remote authenticated users with storm project access to execute arbitrary SQL commands via unspecified vectors.	2009-03-02	6.0	CVE-2008-6383 BID CONFIRM
	Multiple cross-site request forgery (CSRF) vulnerabilities in Comment Mail			CVE-2008

drupal -- comment_mail	5.x before 5.x-1.1, a module for Drupal, allow remote attackers to perform unauthorized actions as administrators via unspecified vectors.	2009-03-02	6.8	CVE-2008-6384 CONFIRM
eric_raymond -- sng	sng_regress in SNG 1.0.2 allows local users to overwrite arbitrary files via a symlink attack on the (1) /tmp/recompiled$$.png, (2) /tmp/decompiled$$.sng, and (3) /tmp/canonicalized$$.sng temporary files.	2009-03-04	6.9	CVE-2008-6398 XF BID MLIST CONFIRM
extrosoft -- thyme	Cross-site scripting (XSS) vulnerability in add_calendars.php in eXtrovert Software Thyme 1.3 allows remote attackers to inject arbitrary web script or HTML via the callback parameter.	2009-03-06	4.3	CVE-2008-6404 XF BID MISC
freedville -- bloghelper	BlogHelper stores common_db.inc under the web root with insufficient access control, which allows remote attackers to download the database file containing user credentials via a direct request.	2009-03-05	5.0	CVE-2009-0826 XF MILW0RM SECUNIA
freedville -- quotebook	QuoteBook stores quotes.inc under the web root with insufficient access control, which allows remote attackers to obtain sensitive database information, including user credentials, via a direct request.	2009-03-05	5.0	CVE-2009-0828 MILW0RM SECUNIA
greensql -- greensql-console	Multiple cross-site scripting (XSS) vulnerabilities in GreenSQL-Console before 0.3.5 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "internal pages."	2009-03-06	4.3	CVE-2008-6416 CONFIRM
greensql -- greensql-console	Unspecified vulnerability in GreenSQL-Console before 0.3.5 allows attackers to obtain the "installation directory" via unknown vectors.	2009-03-06	5.0	CVE-2008-6417 CONFIRM SECUNIA
ibm -- aix	The kernel in IBM AIX 5.2 and 5.3 does not properly handle resizing JFS2 filesystems on concurrent volume groups spread across multiple nodes, which allows local users of one node to cause a denial of service (remote node crash) by using chfs or lreducelv to reduce a filesystem's size.	2009-03-06	4.9	CVE-2008-1594 BID
	Cross-site scripting (XSS) vulnerability in the userranks feature in modules/system/admin.php in			CVE-2008-

impresscms -- impresscms	ImpressCMS 1.0.2 final allows remote attackers to inject arbitrary web script or HTML via the rank_title parameter. NOTE: some of these details are obtained from third party information.	2009-03-02	4.3	6360 CONFIRM SECUNIA
insun_podcast -- feedcms	Directory traversal vulnerability in index.php in InSun Feed CMS 1.7.3 19Beta allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the lang parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-02	6.8	CVE-2008-6361 XF MISC BID
linux -- kernel	The clone system call in the Linux kernel 2.6.28 and earlier allows local users to send arbitrary signals to a parent process from an unprivileged child process by launching an additional child process with the CLONE_PARENT flag, and then letting this new process exit.	2009-02-27	6.3	CVE-2009-0028 CONFIRM MISC MISC SUSE
linux -- kernel	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel 2.6.27 before 2.6.27.19 and 2.6.28 before 2.6.28.7 does not validate the superblock configuration, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) by attempting to mount a crafted ext4 filesystem.	2009-02-27	4.9	CVE-2009-0748 VUPEN CONFIRM CONFIRM CONFIRM CONFIRM
mihai_bazon -- pical	Cross-site scripting (XSS) vulnerability in piCal 0.91h and earlier, a module for XOOPS, allows remote attackers to inject arbitrary web script or HTML via the event_id parameter in index.php.	2009-03-04	4.3	CVE-2009-0805 CONFIRM CONFIRM
mldonkey -- mldonkey	Absolute path traversal vulnerability in MLDonkey 2.8.4 through 2.9.7 allows remote attackers to read arbitrary files via a leading "//" (double slash) in the filename.	2009-03-03	5.0	CVE-2009-0753 MLIST SECUNIA CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.7, Thunderbird before 2.0.0.21, and SeaMonkey before 1.1.15 decodes invisible characters when they are displayed in the location bar, which causes an incorrect address to be	2009-03-04	5.8	CVE-2009-0777 CONFIRM CONFIRM

	displayed and makes it easier for remote attackers to spoof URLs and conduct phishing attacks.			CONFIRM
mozilla -- firefox	Mozilla Firefox 2.0.0.20 and earlier allows remote attackers to cause a denial of service (application crash) via nested calls to the window.print function, as demonstrated by a window.print(window.print()) in the onclick attribute of an INPUT element.	2009-03-04	5.0	CVE-2009-0821 BID MISC
mysql -- mysql	sql/item_xmlfunc.cc in MySQL before 5.1.32 allows remote authenticated users to cause a denial of service (crash) via "an XPath expression employing a scalar expression as a FilterExpr with ExtractValue() or UpdateXML()," which triggers an assertion failure.	2009-03-04	5.0	CVE-2009-0819 CONFIRM
nagios -- nagios	Unspecified vulnerability in Nagios before 3.0.6 has unspecified impact and remote attack vectors related to CGI programs, "adaptive external commands," and "writing newlines and submitting service comments."	2009-03-02	5.0	CVE-2008-6373 CONFIRM CONFIRM
nexusjnr -- jbook	JBook stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request to userids.mdb.	2009-03-02	5.0	CVE-2008-6375 XF MISC
ocean12tech -- contact_manager_pro	Cross-site scripting (XSS) vulnerability in default.asp in Ocean12 Contact Manager Pro 1.02 allows remote attackers to inject arbitrary web script or HTML via the DisplayFormat parameter.	2009-03-02	4.3	CVE-2008-6370 XF BID MILW0RM SECUNIA OSVDB
openbsd -- openbsd	The aspath_prepend function in rde_attr.c in bgpd in OpenBSD 4.3 and 4.4 allows remote attackers to cause a denial of service (application crash) via an Autonomous System (AS) advertisement containing a long AS path.	2009-03-04	5.0	CVE-2009-0780 OPENBSD OPENBSD
opengoo -- opengoo	Unspecified vulnerability in OpenGoo before 1.2.1 allows remote authenticated users to modify their own permissions via unknown attack vectors.	2009-03-04	6.5	CVE-2009-0806 BID
	SQL injection vulnerability in			

php-fusion -- members_cv_module	members.php in the Members CV (job) module 1.0 for PHP-Fusion, when magic_quotes_gpc is disabled, allows remote authenticated users to execute arbitrary SQL commands via the sortby parameter.	2009-03-05	6.0	CVE-2009-0831 BID MILW0RM SECUNIA
phpf1 -- max's_guestbook	Cross-site scripting (XSS) vulnerability in index.php in Max's Guestbook allows remote attackers to inject arbitrary web script or HTML via the (1) name, (2) email, and (3) message parameters.	2009-03-02	4.3	CVE-2008-6359 XF BID BUGTRAQ SECUNIA OSVDB
poppler -- poppler	The FormWidgetChoice::loadDefaults function in Poppler before 0.10.4 allows remote attackers to cause a denial of service (crash) via a PDF file with an invalid Form Opt entry.	2009-03-03	5.0	CVE-2009-0755 MLIST MLIST SECUNIA MLIST CONFIRM
poppler -- poppler	The JBIG2Stream::readSymbolDictSeg function in Poppler before 0.10.4 allows remote attackers to cause a denial of service (crash) via a PDF file that triggers a parsing error, which is not properly handled by JBIG2SymbolDict::~JBIG2SymbolDict and triggers an invalid memory dereference.	2009-03-03	5.0	CVE-2009-0756 MLIST MLIST SECUNIA MLIST CONFIRM
qip -- qip	QIP 2005 build 8082 allows remote attackers to cause a denial of service (CPU consumption and application hang) via a crafted Rich Text Format (RTF) ICQ message, as demonstrated by an {\rtf\pict\&&} message. NOTE: the vulnerability may be in Sergey Tkachenko TRichView. If so, then this should not be treated as a vulnerability in QIP.	2009-03-06	4.3	CVE-2009-0769 BID BUGTRAQ OSVDB SECUNIA
refbase -- refbase	Cross-site scripting (XSS) vulnerability in refbase before 0.9.5 allows remote attackers to inject arbitrary web script or HTML via the headerMsg parameter to (1) show.php and (2) search.php. NOTE: some of these details are obtained from third party information.	2009-03-05	4.3	CVE-2008-6400 BID

scriptsez -- ez_php_comment	Cross-site scripting (XSS) vulnerability in ScriptsEz Ez PHP Comment allows remote attackers to inject arbitrary web script or HTML via the name parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-06	4.3	CVE-2009-0762 BID SECUNIA OSVDB
team5 -- team_board	Team Board 1.x and 2.x stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing credentials via a direct request for data/team.mdb.	2009-03-06	5.0	CVE-2009-0760 OSVDB MILW0RM SECUNIA MISC
team5.team_board -- 1.0 team5.team_board -- 1.0.1 team5.team_board -- 1.0.2 team5.team_board -- 1.0.3 team5.team_board -- 1.0.4 team5.team_board -- 1.0.5	Cross-site scripting (XSS) vulnerability in online.asp in Team Board 1.x allows remote attackers to inject arbitrary web script or HTML via the lookname parameter.	2009-03-06	4.3	CVE-2009-0761 BID MILW0RM
ticklespace -- answers_module	Cross-site scripting (XSS) vulnerability in the Answers module 5.x-1.x-dev and possibly other 5.x versions, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via a Simple Answer to a question.	2009-03-06	4.3	CVE-2008-6413 VUPEN BID FULLDISC CONFIRM
typo3 -- typo3	The jumpUrl mechanism in class.tslib_fe.php in TYPO3 4.0 before 4.0.12, 4.1 before 4.1.10, 4.2 before 4.2.6, and 3.3.x through 3.8.x leaks a hash secret (juHash) in an error message, which allows remote attackers to read arbitrary files by including the hash in a request.	2009-03-04	5.0	CVE-2009-0815 DEBIAN CONFIRM
typo3 -- typo3	Cross-site scripting (XSS) vulnerability in the backend user interface in TYPO3 4.0 before 4.0.12, 4.1 before 4.1.10, 4.2 before 4.2.6, and 3.3.x through 3.8.x allows remote attackers to inject arbitrary web script or HTML via multiple unspecified fields.	2009-03-04	4.3	CVE-2009-0816 CONFIRM
ubuntu -- ubuntu_linux	The dbus request handler in (1) network-manager-applet and (2) NetworkManager in Ubuntu 6.06 LTS, 7.10, 8.04 LTS, and 8.10 does not properly verify privileges, which allows local users to discover (a)	2009-03-04	4.6	CVE-2009-0365 BID

	network connection passwords and (b) pre-shared keys via unspecified queries.			
ubuntu -- ubuntu_linux	network-manager-applet in Ubuntu 8.10 does not properly verify privileges for dbus (1) modify and (2) delete requests, which allows local users to change or remove the network connections of arbitrary users via unspecified vectors.	2009-03-04	6.2	CVE-2009-0578 UBUNTU BID
w3matter -- revsense	Cross-site scripting (XSS) vulnerability in index.php in W3matter RevSense 1.0 allows remote attackers to inject arbitrary web script or HTML via the section parameter.	2009-03-02	4.3	CVE-2008-6385 SECUNIA MISC
yaws -- yaws	Yaws before 1.80 allows remote attackers to cause a denial of service (memory consumption and crash) via a request with a large number of headers.	2009-03-02	5.0	CVE-2009-0751 CONFIRM BID MLIST MILW0RM SECUNIA
znc -- znc	Multiple CRLF injection vulnerabilities in webadmin in ZNC before 0.066 allow remote authenticated users to modify the znc.conf configuration file and gain privileges via CRLF sequences in the quit message and other vectors.	2009-03-03	6.5	CVE-2009-0759 CONFIRM CONFIRM CONFIRM MLIST

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
3ds -- enovia_smarteam ibm -- catia	The Web Editor in Dassault Systemes ENOVIA SmarTeam V5 before Release 18 Service Pack 8, and possibly CATIA and other products, allows remote authenticated users to read the profile card of an object in the document class via a link that is sent from the owner of the document object.	2009-03-04	3.5	CVE-2009-0809 VUPEN BID AIXAPAR SECUNIA
alcovebook -- sgml2x	rlatex in AlcoveBook sgml2x 1.0.0 allows local users to overwrite arbitrary files via a symlink attack on temporary files.	2009-03-04	3.6	CVE-2008-6397 XF BID MLIST CONFIRM
	Cross-site scripting (XSS) vulnerability in the edit account page in the Web Server in Cisco			

cisco -- unified_meetingplace	Unified MeetingPlace Web Conferencing 6.0 before 6.0(517.0) (aka 6.0 MR4) and 7.0 before 7.0(2) (aka 7.0 MR1) allows remote authenticated users to inject arbitrary web script or HTML via the E-mail Address field.	2009-02-27	3.5	CVE-2009-0743 CISCO
drupal -- protected_node_module	Cross-site scripting (XSS) vulnerability in the Protected Node module 5.x before 5.x-1.4 and 6.x before 6.x-1.5, a module for Drupal, allows remote authenticated users with "administer site configuration" permissions to inject arbitrary web script or HTML via the Password page info field, which is not properly handled by the protected_node_enterpassword function in protected_node.module.	2009-03-04	3.5	CVE-2009-0817 VUPEN CONFIRM CONFIRM
drupal -- taxonomy_theme_module	Cross-site scripting (XSS) vulnerability in the taxonomy_theme_admin_table_builder function (taxonomy_theme_admin.inc) in Taxonomy Theme module before 5.x-1.2, a module for Drupal, allows remote authenticated users with the "administer taxonomy" permission, or the ability to create pages when tagging is enabled, to inject arbitrary web script or HTML via the Vocabulary name (name parameter) to index.php. NOTE: some of these details are obtained from third party information.	2009-03-04	3.5	CVE-2009-0818 BID CONFIRM
opensc-project -- opensc	OpenSC before 0.11.7 allows physically proximate attackers to bypass intended PIN requirements and read private data objects via a (1) low level APDU command or (2) debugging tool, as demonstrated by reading the 4601 or 4701 file with the opensc-explorer or opensc-tool program.	2009-03-02	2.1	CVE-2009-0368 BID MLIST
php -- php	PHP 4.4.4, 5.1.6, and other versions, when running on Apache, allows local users to modify behavior of other sites hosted on the same web server by modifying the mbstring.func_overload setting within .htaccess, which causes this setting to be applied to other virtual hosts on the same server.	2009-03-03	2.1	CVE-2009-0754 MLIST MLIST MLIST CONFIRM

Back to top