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
deeemm -- DMCMS	SQL injection vulnerability in index.php in DeeEmm CMS (DMCMS) 0.7.4 allows remote attackers to execute arbitrary SQL commands via the page parameter. NOTE: the id vector is already covered by CVE-2007-5679.	unknown 2008-08-20	7.5	CVE-2008-3720 MILW0RM XF
deeemm -- DMCMS	PHP remote file inclusion vulnerability in user_language.php in DeeEmm CMS (DMCMS) 0.7.4 allows remote attackers to execute arbitrary PHP code via a URL in the language_dir parameter.	unknown 2008-08-20	7.5	CVE-2008-3721 MILW0RM XF
discountedscripts -- quick_poll_script	SQL injection vulnerability in code.php in Quick Poll Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3765 OTHER-REF BID XF
echovnc -- echovnc	Stack-based buffer overflow in the CLogger::WriteFormated function in echoware/Logger.cpp in EchoVNC Linux before 1.1.2 allows remote echoServers to execute arbitrary code via a large (1) group or (2) user list, aka a "very crowded echoServer" attack. NOTE: some of these details are obtained from third party information.	unknown 2008-08-19	7.5	CVE-2008-3705 OTHER-REF BID
eo-video -- eo-video	Stack-based buffer overflow in EO Video (eo-video) 1.36 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a .eop (aka playlist) file with a ProjectElement element that contains a long Name element.	unknown 2008-08-20	9.3	CVE-2008-3733 MILW0RM BID XF
fipsASP -- fipsCMS	SQL injection vulnerability in forum/neu.asp in fipsCMS 2.1 allows remote attackers to execute arbitrary SQL commands via the kat parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-20	7.5	CVE-2008-3722 OTHER-REF BID XF
GNOME -- gnome GNOME -- yelp	Format string vulnerability in the window_error function in yelp-window.c in yelp in Gnome after 2.19.90 and before 2.24 allows remote attackers to execute arbitrary code via format string specifiers in an invalid URI on the command line, as demonstrated by use of yelp within (1) man or (2) ghelp URI handlers in Firefox, Evolution, and unspecified other programs.	unknown 2008-08-18	10.0	CVE-2008-3533 OTHER-REF BID XF
Hotscripts -- cyboards_php_lite	Multiple PHP remote file inclusion vulnerabilities in CyBoards PHP Lite 1.21 allow remote attackers to execute arbitrary PHP code via a URL in the script_path parameter to (1) flat_read.php, (2) post.php, (3) process_post.php, (4) process_search.php, (5) forum.php, (6) process_subscribe.php, (7) read.php, (8) search.php, (9) subscribe.php in path/; and (10) add_ban.php, (11) add_ban_form.php, (12) add_board.php, (13) add_vip.php, (14) add_vip_form.php, (15) copy_ban.php, (16) copy_vip.php, (17) delete_ban.php, (18) delete_board.php, (19) delete_messages.php,	unknown 2008-08-19	7.5	CVE-2008-3707 OTHER-REF VIM BID XF

	(20) delete_vip.php, (21) edit_ban.php, (22) edit_board.php, (23) edit_vip.php, (24) index.php, (25) lock_messages.php, (26) login.php, (27) modify_ban_list.php, (28) modify_vip_list.php, (29) move_messages.php, (30) process_add_board.php, (31) process_ban.php, (32) process_delete_ban.php, (33) process_delete_board.php, (34) process_delete_messages.php, (35) process_delete_vip.php, (36) process_edit_board.php, (37)! process_lock_messages.php, (38) process_login.php, (39) process_move_messages.php, (40) process_sticky_messages.php, (41) process_vip.php, and (42) sticky_messages.php in path/adminopts. NOTE: the include/common.php vector is covered by CVE-2006-2871. NOTE: some of these vectors might not be vulnerabilities under proper installation.			
Ipswitch -- ws_ftp_home Ipswitch -- WS_FTP Pro	Format string vulnerability in Ipswitch WS_FTP Home 2007.0.0.2 and WS_FTP Professional 2007.1.0.0 allows remote FTP servers to cause a denial of service (application crash) or possibly execute arbitrary code via format string specifiers in a connection greeting (response).	unknown 2008-08-20	9.3	CVE-2008-3734 MILW0RM BID XF
lbstone -- active_php_bookmarks lbstone -- apb	SQL injection vulnerability in view_group.php in Active PHP Bookmarks (APB) 1.1.02 and 1.2.06 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3748 MILW0RM BID
Linux -- Kernel	Integer overflow in the dccp_setsockopt_change function in net/dccp/proto.c in the Datagram Congestion Control Protocol (DCCP) subsystem in the Linux kernel 2.6.17-rc1 through 2.6.26.2 allows remote attackers to cause a denial of service (panic) via a crafted integer value, related to Change L and Change R options without at least one byte in the dccpsf_val field.	unknown 2008-08-18	7.1	CVE-2008-3276 MLIST OTHER-REF BID
Lussumo -- Vanilla	Cross-site request forgery (CSRF) vulnerability in ajax/UpdateCheck.php in Vanilla 1.1.4 and earlier has unknown impact and remote attack vectors.	unknown 2008-08-21	7.5	CVE-2008-3759 OTHER-REF OTHER-REF OTHER-REF
Microsoft -- Visual Studio	Stack-based buffer overflow in the MaskedEdit ActiveX control in Msmask32.ocx 6.0.81.69, and possibly other versions before 6.0.84.18, in Microsoft Visual Studio 6.0 allows remote attackers to execute arbitrary code via a long Mask parameter, as exploited in the wild in August 2008. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-18	9.3	CVE-2008-3704 BID
MicroWorld Technologies -- mailscan	Web Based Administration in MicroWorld Technologies MailScan 5.6.a espatch 1 allows remote attackers to bypass authentication and obtain administrative access via a direct request with (1) an IsAdmin=true cookie value or (2) no cookie.	unknown 2008-08-20	7.5	CVE-2008-3729 BUGTRAQ OTHER-REF XF
openwsman -- openwsman	The client in Openwsman 1.2.0 and 2.0.0, in unknown configurations, allows remote Openwsman servers to replay SSL sessions via unspecified vectors.	unknown 2008-08-18	7.5	CVE-2008-2233 BID
openwsman -- openwsman	Multiple buffer overflows in Openwsman 1.2.0 and 2.0.0 allow remote attackers to execute arbitrary code via a crafted "Authorization: Basic" HTTP header.	unknown 2008-08-18	7.5	CVE-2008-2234 SUSE BID
Papoo -- Papoo	SQL injection vulnerability in index.php in Papoo before 3.7.2 allows remote attackers to execute arbitrary SQL commands via the suchanzahl parameter.	unknown 2008-08-20	7.5	CVE-2008-3724
party_gaming -- party_poker_client	The PartyGaming PartyPoker client program 121/120 does not properly verify the authenticity of updates, which allows remote man-in-the-middle attackers to execute arbitrary code via a Trojan horse update.	unknown 2008-08-18	7.6	CVE-2008-3324 FULLDISC BID
phpArcadeScript -- phpArcadeScript	SQL injection vulnerability in index.php in PHPArcadeScript (PHP Arcade Script) 4.0 allows remote attackers to execute arbitrary SQL commands via the cat parameter in a browse action.	unknown 2008-08-19	7.5	CVE-2008-3711 MILW0RM BID
phpbasket -- phpbasket	SQL injection vulnerability in product.php in PHPBasket allows remote attackers to execute arbitrary SQL commands via the pro_id parameter.	unknown 2008-08-19	7.5	CVE-2008-3713 MILW0RM BID

scripts-for-sites -- affiliate_directory	SQL injection vulnerability in directory.php in SFS Affiliate Directory allows remote attackers to execute arbitrary SQL commands via the id parameter in a deadlink action.	unknown 2008-08-20	7.5	CVE-2008-3719 OTHER-REF BID
Symantec -- Veritas Storage Foundation	The management console in the Volume Manager Scheduler Service (aka VxSchedService.exe) in Symantec Veritas Storage Foundation for Windows (SFW) 5.0, 5.0 RP1a, and 5.1 accepts NULL NTLMSSP authentication, which allows remote attackers to execute arbitrary code via requests to the service socket that create "snapshots schedules" registry values specifying future command execution. NOTE: this issue exists because of an incomplete fix for CVE-2007-2279.	unknown 2008-08-18	10.0	CVE-2008-3703 BUGTRAQ BUGTRAQ OTHER-REF OTHER-REF BID SECTRACK SECUNIA XF
turnkeywebtools -- php_live_helper	SQL injection vulnerability in onlinestatus_html.php in Turnkey PHP Live Helper 2.0.1 and earlier allows remote attackers to execute arbitrary SQL commands via the dep parameter, related to lack of input sanitization in the get function in global.php.	unknown 2008-08-21	7.5	CVE-2008-3762 BUGTRAQ MILW0RM OTHER-REF BID
turnkeywebtools -- php_live_helper	Eval injection vulnerability in chat.php in Turnkey PHP Live Helper 2.0.1 and earlier allows remote attackers to execute arbitrary PHP code via the test parameter, and probably arbitrary parameters.	unknown 2008-08-21	7.5	CVE-2008-3764 BUGTRAQ MILW0RM OTHER-REF OTHER-REF BID
VideoLAN -- VLC Media Player	Integer overflow in the Open function in modules/demux/tta.c in VLC Media Player 0.8.6i allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted TTA file, which triggers a heap-based buffer overflow. NOTE: some of these details are obtained from third party information.	unknown 2008-08-20	9.3	CVE-2008-3732 MILW0RM OTHER-REF BID XF
YourFreeWorld -- ad_board_script	SQL injection vulnerability in trr.php in YourFreeWorld Ad Board Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-20	7.5	CVE-2008-3725 OTHER-REF BID
YourFreeWorld -- banner_management_script	SQL injection vulnerability in tr.php in Banner Management Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3749 MILW0RM BID
YourFreeWorld -- url_rotator_script	SQL injection vulnerability in tr.php in YourFreeWorld URL Rotator Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3750 OTHER-REF BID
YourFreeWorld -- Short Url and Url Tracker Script	SQL injection vulnerability in tr.php in YourFreeWorld Short Url & Url Tracker Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3751 OTHER-REF BID
YourFreeWorld -- ad-exchange_script	SQL injection vulnerability in tr.php in YourFreeWorld Ad-Exchange Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3752 OTHER-REF BID
YourFreeWorld -- programs_rating_script	SQL injection vulnerability in details.php in YourFreeWorld Programs Rating Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3753 OTHER-REF BID
YourFreeWorld -- Stylish Text Ads Script	SQL injection vulnerability in trl.php in YourFreeWorld Stylish Text Ads Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3754 OTHER-REF BID
YourFreeWorld -- classifieds	SQL injection vulnerability in view.php in YourFreeWorld Classifieds Script allows remote attackers to execute arbitrary SQL commands via the category parameter.	unknown 2008-08-21	7.5	CVE-2008-3755 OTHER-REF BID
YourFreeWorld -- viral_marketing_script	SQL injection vulnerability in tr.php in YourFreeWorld Viral Marketing Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3756 OTHER-REF BID
YourFreeWorld -- forced_matrix_script	SQL injection vulnerability in tr1.php in YourFreeWorld Forced Matrix Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-21	7.5	CVE-2008-3757 OTHER-REF BID

zeeways -- zeejobsite	SQL injection vulnerability in bannerclick.php in ZEEJOBSITE 2.0 allows remote attackers to execute arbitrary SQL commands via the adid parameter.	unknown 2008-08-19	7.5	CVE-2008-3706 MILW0RM BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
AWStats -- AWStats	Cross-site scripting (XSS) vulnerability in awstats.pl in AWStats 6.8 allows remote attackers to inject arbitrary web script or HTML via the query_string, a different vulnerability than CVE-2006-3681 and CVE-2006-1945.	unknown 2008-08-19	4.3	CVE-2008-3714 OTHER-REF OTHER-REF
cyberbb -- cyberbb	Multiple SQL injection vulnerabilities in cyberBB 0.6 allow remote authenticated users to execute arbitrary SQL commands via the (1) id parameter to show_topic.php and the (2) user parameter to profile.php.	unknown 2008-08-20	6.5	CVE-2008-3718 MILW0RM BID XF
dotcms -- dotcms	Multiple directory traversal vulnerabilities in dotCMS 1.6.0.9 allow remote attackers to read arbitrary files via a .. (dot dot) in the id parameter to (1) news/index.dot and (2) getting_started/macros/macros_detail.dot.	unknown 2008-08-19	4.3	CVE-2008-3708 MILW0RM BID XF
harmoni -- harmoni	Cross-site request forgery (CSRF) vulnerability in Harmoni before 1.6.0 allows remote attackers to make administrative modifications via a (1) save or (2) delete action to an unspecified component.	unknown 2008-08-19	6.0	CVE-2008-3716 OTHER-REF OTHER-REF XF
harmoni -- harmoni	Harmoni before 1.6.0 does not require administrative privileges to list (1) user names or (2) asset ids, which allows remote attackers to obtain sensitive information.	unknown 2008-08-19	5.0	CVE-2008-3717 OTHER-REF OTHER-REF BID XF
Hotscripts -- cyboards_php_lite	Multiple cross-site scripting (XSS) vulnerabilities in CyBoards PHP Lite 1.21 allow remote attackers to inject arbitrary web script or HTML via the (1) lOptionsOptions, (2) lNavAdminOptions, or (3) lNavReturn parameter to options.php; or the (4) lNavReturn parameter to subscribe.php.	unknown 2008-08-19	4.3	CVE-2008-3709 OTHER-REF VIM BID XF
Hotscripts -- cyboards_php_lite	Multiple directory traversal vulnerabilities in CyBoards PHP Lite 1.21 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the (1) script_path parameter to (a) options.php and the (2) lang_code parameter to (b) copy_vip.php and (c) process_edit_board.php in adminopts/. NOTE: some of these vectors might not be vulnerabilities under proper installation.	unknown 2008-08-19	5.1	CVE-2008-3710 OTHER-REF VIM BID XF
Lussumo -- Vanilla	Multiple cross-site scripting (XSS) vulnerabilities in Lussumo Vanilla 1.1.4 and earlier (1) allow remote attackers to inject arbitrary web script or HTML via the NewPassword parameter to people.php, and allow remote authenticated users to inject arbitrary web script or HTML via the (2) Account picture and (3) Icon fields in account.php. NOTE: some of these details are obtained from third party information.	unknown 2008-08-21	4.3	CVE-2008-3758 BUGTRAQ OTHER-REF OTHER-REF BID
Lussumo -- Vanilla	Cross-site request forgery (CSRF) vulnerability in the sign-out page in Vanilla 1.1.4 and earlier allows remote attackers to trigger the logout of other users via a link or IMG tag to the SignOutNow action in people.php.	unknown 2008-08-21	4.3	CVE-2008-3760 OTHER-REF OTHER-REF OTHER-REF OTHER-REF
Mambo -- Mambo	Multiple cross-site scripting (XSS) vulnerabilities in Mambo 4.6.2 and 4.6.5, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the (1) query string to mambots/editors/mostlyce/jscripts/tiny_mce/filemanager/connectors/php/connector.php and the (2) mosConfig_sitename parameter to administrator/popups/index3pop.php.	unknown 2008-08-19	4.3	CVE-2008-3712 BUGTRAQ BID
MicroWorld Technologies -- mailscan	Cross-site scripting (XSS) vulnerability in Web Based Administration in MicroWorld Technologies MailScan 5.6.a espatch 1 allows remote attackers to inject arbitrary web script or HTML via the URI.	unknown 2008-08-20	4.3	CVE-2008-3726 BUGTRAQ OTHER-REF BID XF

MicroWorld Technologies -- mailscan	Directory traversal vulnerability in Web Based Administration in MicroWorld Technologies MailScan 5.6.a espatch 1 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	unknown 2008-08-20	5.0	CVE-2008-3727 BUGTRAQ OTHER-REF BID XF
MicroWorld Technologies -- mailscan	Web Based Administration in MicroWorld Technologies MailScan 5.6.a espatch 1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to determine the installation path, IP addresses, and error messages via direct requests to files under LOG/.	unknown 2008-08-20	5.0	CVE-2008-3728 BUGTRAQ OTHER-REF BID XF
nordicwind -- document management system nordicwind -- NOAH	Cross-site scripting (XSS) vulnerability in Nordicwind Document Management System (NOAH) before 3.2.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-08-20	4.3	CVE-2008-3730 OTHER-REF
phpizabi -- phpizabi	Directory traversal vulnerability in index.php in PHPizabi 0.848b C1 HFP3 allows remote authenticated administrators to read arbitrary files via (1) a .. (dot dot), (2) a URL, or possibly (3) a full pathname in the id parameter in an admin.templates.edittemplate action. NOTE: some of these details are obtained from third party information.	unknown 2008-08-20	6.3	CVE-2008-3723 OTHER-REF OTHER-REF BID XF
phpizabi -- phpizabi	Cross-site scripting (XSS) vulnerability in index.php in PHPizabi before 848 Core HotFix Pack 3 allows remote attackers to inject arbitrary web script or HTML via the query parameter in a blogs.search action.	unknown 2008-08-20	4.3	CVE-2008-3735 OTHER-REF OTHER-REF
postfix -- postfix	Postfix before 2.3.15, 2.4 before 2.4.8, 2.5 before 2.5.4, and 2.6 before 2.6-20080814, when the operating system supports hard links to symlinks, allows local users to append e-mail messages to a file to which a root-owned symlink points, by creating a hard link to this symlink and then sending a message. NOTE: this can be leveraged to gain privileges if there is a symlink to an init script.	unknown 2008-08-18	6.2	CVE-2008-2936 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF OTHER-REF SUSE XF
serv-u -- serv-u_file_server	Unspecified vulnerability in Serv-U File Server 7.x before 7.2.0.1 allows remote authenticated users to cause a denial of service (daemon crash) via an SSH session with SFTP commands for directory creation and logging.	unknown 2008-08-20	4.0	CVE-2008-3731 OTHER-REF BID XF
turnkeywebtools -- php_live_helper	Variable overwrite vulnerability in libsecure.php in Turnkey PHP Live Helper 2.0.1 and earlier, when register_globals is enabled, allows remote attackers to overwrite arbitrary variables related to the db config file. NOTE: this can be leveraged for code injection by overwriting the language file.	unknown 2008-08-21	6.8	CVE-2008-3763 BUGTRAQ MILW0RM OTHER-REF OTHER-REF BID
VMWare -- VMWare Workstation	hcmon.sys in VMware Workstation 6.0.0.45731 uses the METHOD_NEITHER communication method for IOCTLs, which has an unknown impact (possibly crash) and local attack vectors via a crafted IOCTL request.	unknown 2008-08-21	4.9	CVE-2008-3761 MILW0RM OTHER-REF BID SECTRACK XF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
flexcms -- flexcms	Cross-site scripting (XSS) vulnerability in inc-core-admin-editor-previouscolorsjs.php in the FlexCMS 2.5 and earlier, when register_globals is enabled, allows remote attackers to inject arbitrary web script or HTML via the PreviousColorsString parameter.	unknown 2008-08-19	2.6	CVE-2008-3715 BUGTRAQ BID

postfix -- postfix	Postfix 2.5 before 2.5.4 and 2.6 before 2.6-20080814 delivers to a mailbox file even when this file is not owned by the recipient, which allows local users to read e-mail messages by creating a mailbox file corresponding to another user's account name.	unknown 2008-08-18	1.9	CVE-2008-2937 OTHER-REF OTHER-REF SUSE XF
redhat -- enterprise_linux	yum-rhn-plugin in Red Hat Enterprise Linux (RHEL) 5 does not verify the SSL certificate for a file download from a Red Hat Network (RHN) server, which makes it easier for remote man-in-the-middle attackers to cause a denial of service (loss of updates) or force the download and installation of official Red Hat packages that were not requested.	unknown 2008-08-18	2.6	CVE-2008-3270 OTHER-REF REDHAT BID SECTRACK

Back to top