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	Sour
alphadmin -- alphadmin_cms	AlphAdmin CMS 1.0.5/03 allows remote attackers to bypass authentication and gain administrative access by setting the aa_login cookie value to 1. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	7.5	CVE
AlstraSoft -- Affiliate Network Pro	SQL injection vulnerability in index.php in AlstraSoft Affiliate Network Pro allows remote attackers to execute arbitrary SQL commands via the pgm parameter in a directory action.	unknown 2008-07-21	7.5	CVE M
aprox -- aprox_cms_engine aprox -- aproxengine	SQL injection vulnerability in index.php in AproxEngine	unknown 2008-07-24	7.5	CVE M

	(aka Aprox CMS Engine) 5.1.0.4 allows remote attackers to execute arbitrary SQL commands via the id parameter.			OT
arctictracker -- arctic_issue_tracker	SQL injection vulnerability in index.php in Arctic Issue Tracker 2.0.0 allows remote attackers to execute arbitrary SQL commands via the filter parameter.	unknown 2008-07-21	7.5	CVE MI
Asterisk -- Asterisk	Asterisk allows remote attackers to cause a denial of service (CPU consumption) by quickly sending a large number of IAX POKE requests.	unknown 2008-07-22	7.8	CVE OT
Asterisk -- AsteriskNOW Asterisk -- Asterisk Business Edition Asterisk -- Asterisk Appliance Developer Kit Asterisk -- Open Source	The FWDOWNL firmware-download implementation in Asterisk Open Source 1.0.x, 1.2.x before 1.2.30, and 1.4.x before 1.4.21.2; Business Edition A.x.x, B.x.x before B.2.5.4, and C.x.x before C.1.10.3; AsteriskNOW; Appliance Developer Kit 0.x.x; and s800i 1.0.x before 1.2.0.1 allows remote attackers to cause a denial of service (traffic amplification) via an IAX2 FWDOWNL request.	unknown 2008-07-24	7.8	CVE OT
cable-modems -- phphoo3	SQL injection vulnerability in phpHoo3.php in phpHoo3 4.3.9, 4.3.10, 4.4.8, and 5.2.6 allows remote attackers to execute arbitrary SQL commands via the viewCat parameter.	unknown 2008-07-21	7.5	CVE MI
Drupal -- Drupal	Session fixation vulnerability in Drupal 5.x before 5.8 and 6.x before 6.3, when contributed modules "terminate the current request during a login event," allows remote attackers to hijack web	unknown 2008-07-18	7.5	CVE OT

	sessions via unknown vectors.			
eSyndicat -- esyndicat	eSyndiCat 1.6 allows remote attackers to bypass authentication and gain administrative access by setting the admin_lng cookie value to 1. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	7.5	CVE
Fedora -- newsx	Stack-based buffer overflow in the read_article function in getarticle.c in newsx 1.6 allows remote attackers to execute arbitrary code via a news article containing a large number of lines starting with a period.	unknown 2008-07-21	10.0	CVE F F
iamilkay -- yuhhu_pubs_black_cat	SQL injection vulnerability in browse.groups.php in Yuhhu Pubs Black Cat allows remote attackers to execute arbitrary SQL commands via the category parameter.	unknown 2008-07-18	7.5	CVE BU
Linux -- Kernel	The LDT implementation in the Linux kernel 2.6.25.x on x86_64 platforms uses an incorrect size for ldt_desc, which allows local users to cause a denial of service (system crash) or possibly gain privileges via unspecified vectors.	unknown 2008-07-24	7.2	CVE OT
MojoScripts -- mojojobs	SQL injection vulnerability in mojoJobs.cgi in MojoJobs allows remote attackers to execute arbitrary SQL commands via the cat_a parameter.	unknown 2008-07-24	7.5	CVE M
Oracle -- weblogic_server BEA Systems -- WebLogic Server BEA Systems -- apache_connector_in_weblogic_server	Stack-based buffer overflow in the Apache Connector (mod_wl) in Oracle WebLogic Server (formerly BEA WebLogic Server) 10.3 and earlier allows remote	unknown 2008-07-22	10.0	CVE M SE

	attackers to execute arbitrary code via a long HTTP version string, as demonstrated by a string after "POST /.jsp" in an HTTP request. NOTE: it is possible that this overlaps CVE-2008-2579 or another issue disclosed in Oracle's CPUJul2008 advisory.			
ppmate -- ppmedia_class	Heap-based buffer overflow in the PPMedia Class ActiveX control in PPMPlayer.dll in PPMate 2.3.1.93 allows remote attackers to execute arbitrary code via a long argument to the StartUrl method. NOTE: some of these details are obtained from third party information.	unknown 2008-07-21	10.0	CVE M
pragyan -- praygan_cms	PHP remote file inclusion vulnerability in cms/modules/form.lib.php in Pragyan CMS 2.6.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the (1) sourceFolder or (2) moduleFolder parameter.	unknown 2008-07-18	9.3	CVE M
RIM -- blackberry_enterprise_server_for_exchange RIM -- blackberry_enterprise_server_for_domino Blackberry -- enterprise_server RIM -- blackberry_enterprise_server_for_novell_groupwise Blackberry -- unite RIM -- Blackberry Enterprise Server RIM -- blackberry_unite	Unspecified vulnerability in the PDF distiller component in the BlackBerry Attachment Service in BlackBerry Unite! 1.0 SP1 (1.0.1) before bundle 36 and BlackBerry Enterprise Server 4.1 SP3 (4.1.3) through 4.1 SP5 (4.1.5) allows user-assisted remote attackers to execute arbitrary code via a crafted PDF file attachment.	unknown 2008-07-21	9.3	CVE OT OT C SE Sl
Siteframe -- siteframe_cms Siteframe -- Siteframe Beaumont	SQL injection vulnerability in folder.php in Siteframe CMS 3.2.3 and earlier, and Siteframe Beaumont 5.0.5 and earlier, allows remote	unknown 2008-07-22	7.5	CVE M

	attackers to execute arbitrary SQL commands via the id parameter.			
Social Engine -- Social Engine	Multiple SQL injection vulnerabilities in SocialEngine (SE) before 2.83 allow remote attackers to execute arbitrary SQL commands via (1) an se_user cookie to include/class_user.php or (2) an se_admin cookie to include/class_admin.php.	unknown 2008-07-25	7.5	CVE BU
Softacid -- hotel_reservation_system_multi	SQL injection vulnerability in picture_pic_bv.asp in SoftAcid Hotel Reservation System (HRS) Multi allows remote attackers to execute arbitrary SQL commands via the key parameter.	unknown 2008-07-24	7.5	CVE MI
TPL Design -- tplsoccersite	Multiple SQL injection vulnerabilities in tplSoccerSite 1.0 allow remote attackers to execute arbitrary SQL commands via (1) the opp parameter to tampereunited/opponent.php; or the id parameter to (2) index.php, (3) player.php, (4) matchdetails.php, or (5) additionalpage.php in tampereunited/.	unknown 2008-07-21	7.5	CVE MI
ultrastats -- ultrastats	SQL injection vulnerability in players-detail.php in UltraStats 0.2.136, 0.2.140, and 0.2.142 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-21	7.5	CVE MI OT
XOOPS -- Xoops	Directory traversal vulnerability in modules/system/admin.php in XOOPS 2.0.18 1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the fct parameter. NOTE: the provenance of this	unknown 2008-07-25	7.5	CVE

	information is unknown; the details are obtained solely from third party information.			
Zoph -- Zoph	Multiple SQL injection vulnerabilities in Zoph before 0.7.0.5 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2008-07-22	7.5	CVE OT

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
alain_barbet -- filesys_smbclientparser	The Filesys::SmbClientParser module 2.7 and earlier for Perl allows remote SMB servers to execute arbitrary code via a folder name containing shell metacharacters.	unknown 2008-07-24	6.8	CVE-2008-3285 BUGTRAQ BID XF
BrickHost -- phpScheduleIt	Unspecified vulnerability in phpScheduleIt 1.2.0 through 1.2.9, when useLogonName is enabled, allows remote attackers with administrator email address knowledge to bypass restrictions and gain privileges via unspecified vectors related to login names. NOTE: some of these details are obtained from third party information.	unknown 2008-07-24	6.8	CVE-2008-3268 OTHER-REF BID XF
Carlos Desseno -- youtube_blog	Cross-site scripting (XSS) vulnerability in mensaje.php in C. Desseno YouTube Blog (ytb) 0.1 allows remote attackers to inject arbitrary web script or HTML via the m parameter.	unknown 2008-07-25	4.3	CVE-2008-3305 MILW0RM BID XF
Citrix -- xenserver	Cross-site scripting (XSS) vulnerability in the XenAPI HTTP interfaces in Citrix XenServer Express, Standard, and Enterprise Edition 4.1.0; Citrix XenServer Dell Edition (Express and Enterprise) 4.1.0; and HP integrated Citrix XenServer (Select and Enterprise) 4.1.0 allows remote attackers to	unknown 2008-07-22	4.3	CVE-2008-3253 OTHER-REF BID SECTRACK XF

	inject arbitrary web script or HTML via unspecified vectors.			
Clam Anti-Virus -- ClamAV	libclamav/petite.c in ClamAV before 0.93.3 allows remote attackers to cause a denial of service via a malformed Petite file that triggers an out-of-bounds memory access. NOTE: this issue exists because of an incomplete fix for CVE-2008-2713.	unknown 2008-07-18	5.0	CVE-2008-3215 MLIST MLIST OTHER-REF OTHER-REF
Claroline -- Claroline	Multiple cross-site scripting (XSS) vulnerabilities in Claroline before 1.8.10 allow remote attackers to inject arbitrary web script or HTML via (1) the cwd parameter in a rqMkHtml action to document/rqmkhtml.php, or the query string to (2) announcements/announcements.php, (3) calendar/agenda.php, (4) course/index.php, (5) course_description/index.php, (6) document/document.php, (7) exercise/exercise.php, (8) group/group_space.php, (9) phpbb/newtopic.php, (10) phpbb/reply.php, (11) phpbb/viewtopic.php, (12) wiki/wiki.php, or (13) work/work.php in claroline/.	unknown 2008-07-22	4.3	CVE-2008-3260 BUGTRAQ OTHER-REF OTHER-REF BID XF
Claroline -- Claroline	Open redirect vulnerability in claroline/redirector.php in Claroline before 1.8.10 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the url parameter.	unknown 2008-07-22	4.3	CVE-2008-3261 BUGTRAQ OTHER-REF OTHER-REF BID XF
Claroline -- Claroline	Cross-site request forgery (CSRF) vulnerability in Claroline before 1.8.10 allows remote attackers to change passwords, related to lack of a requirement for the previous password.	unknown 2008-07-22	5.8	CVE-2008-3262 BUGTRAQ OTHER-REF OTHER-REF XF
Debian -- projectl	The save function in br/prefmanager.d in projectl 1.001 creates a projectL.prf file in the current working directory, which allows local users to overwrite	unknown 2008-07-18	4.6	CVE-2008-3216 MLIST OTHER-REF

	arbitrary files via a symlink attack.			
Drupal -- Drupal	Multiple cross-site scripting (XSS) vulnerabilities in Drupal 6.x before 6.3 allow remote attackers to inject arbitrary web script or HTML via vectors related to (1) free tagging taxonomy terms, which are not properly handled on node preview pages, and (2) unspecified OpenID values.	unknown 2008-07-18	4.3	CVE-2008-3218 MLIST OTHER-REF
Drupal -- Drupal	The Drupal filter_xss_admin function in 5.x before 5.8 and 6.x before 6.3 does not "prevent use of the object HTML tag in administrator input," which has unknown impact and attack vectors, probably related to an insufficient cross-site scripting (XSS) protection mechanism.	unknown 2008-07-18	5.0	CVE-2008-3219 MLIST
EMC -- dantz_retrospect_backup_server	The Server Authentication Module in EMC Dantz Retrospect Backup Server 7.5.508 uses a "weak hash algorithm," which makes it easier for context-dependent attackers to recover passwords.	unknown 2008-07-24	5.0	CVE-2008-3288 BUGTRAQ OTHER-REF
EMC Dantz -- Retrospect Backup Client	retroclient.exe in EMC Dantz Retrospect Backup Client 7.5.116 allows remote attackers to cause a denial of service (daemon crash) via malformed packets to TCP port 497, which trigger a NULL pointer dereference.	unknown 2008-07-24	5.0	CVE-2008-3287 BUGTRAQ BID
EMC Dantz -- Retrospect Backup Client	EMC Dantz Retrospect Backup Client 7.5.116 sends the password hash in cleartext at an unspecified point, which allows remote attackers to obtain sensitive information via a crafted packet.	unknown 2008-07-24	5.8	CVE-2008-3289 BUGTRAQ OTHER-REF
EMC Dantz -- Retrospect Backup Client	retroclient.exe in EMC Dantz Retrospect Backup Client 7.5.116 allows remote attackers to cause a denial of service (daemon crash) via a series of long packets containing 0x00 characters to TCP port 497 that trigger memory corruption, probably involving an English product version on a Chinese OS version.	unknown 2008-07-24	5.0	CVE-2008-3290 BUGTRAQ BID

EZWebAlbum -- EZWebAlbum	constants.inc in EZWebAlbum 1.0 allows remote attackers to bypass authentication and gain administrator privileges by setting the photoalbumadmin cookie, as demonstrated via addpage.php.	unknown 2008-07-24	6.4	CVE-2008-3292 MILW0RM BID XF
EZWebAlbum -- EZWebAlbum	Directory traversal vulnerability in download.php in EZWebAlbum allows remote attackers to read arbitrary files via the dlfilename parameter.	unknown 2008-07-24	5.0	CVE-2008-3293 MILW0RM BID XF
F-Prot -- F-Prot Antivirus F-Prot -- scanning_engine	Multiple unspecified vulnerabilities in the scanning engine before 4.4.4 in F-Prot Antivirus before 6.0.9.0 allow remote attackers to cause a denial of service via (1) a crafted UPX-compressed file, which triggers an engine crash; (2) a crafted Microsoft Office file, which triggers an infinite loop; or (3) an ASPack-compressed file, which triggers an engine crash.	unknown 2008-07-21	4.3	CVE-2008-3243 OTHER-REF BID
F-Prot -- F-Prot Antivirus F-Prot -- scanning_engine	The scanning engine before 4.4.4 in F-Prot Antivirus before 6.0.9.0 allows remote attackers to cause a denial of service (engine crash) via a CHM file with a large nb_dir value that triggers an out-of-bounds read.	unknown 2008-07-21	4.3	CVE-2008-3244 OTHER-REF OTHER-REF BID SECTRACK XF
Joomla -- com_dtregister	SQL injection vulnerability in the DT Register (com_dtregister) 2.2.3 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the eventId parameter in a pay_options action to index.php.	unknown 2008-07-24	6.8	CVE-2008-3265 MILW0RM OTHER-REF BID XF
Lenovo -- thinkvantage_system_update	The client in Lenovo System Update before 3.14 does not properly validate the certificate when establishing an SSL connection, which allows remote attackers to install arbitrary packages via an SSL certificate whose X.509 headers match a public certificate used by IBM.	unknown 2008-07-21	5.1	CVE-2008-3249 OTHER-REF
ln-lab -- webproxy	Cross-site scripting (XSS) vulnerability in LunarNight Laboratory WebProxy 1.7.8 and earlier allows remote attackers to	unknown 2008-07-22	4.3	CVE-2008-3255 OTHER-REF OTHER-REF BID

	inject arbitrary web script or HTML via unspecified vectors.			XF
opensuse -- libxcrypt	libxcrypt in SUSE openSUSE 11.0 uses the DES algorithm when the configuration specifies the MD5 algorithm, which makes it easier for attackers to conduct brute-force attacks against hashed passwords.	unknown 2008-07-22	6.2	CVE-2008-3188
precoc -- precms	SQL injection vulnerability in index.php in preCMS 1 allows remote attackers to execute arbitrary SQL commands via the id parameter in a UserProfil action.	unknown 2008-07-22	6.8	CVE-2008-3254 MILW0RM BID XF
Sierra -- SWAT 4	SWAT 4 1.1 and earlier allows remote attackers to cause a denial of service (daemon crash) via a (1) VERIFYCONTENT or (2) GAMECONFIG command sent to the server before user session initialization, which triggers a NULL pointer dereference; or (3) a GAMESPYRESPONSE command followed by a long RS string.	unknown 2008-07-24	5.0	CVE-2008-3286 OTHER-REF OTHER-REF BID XF XF
Social Engine -- Social Engine	SocialEngine (SE) before 2.83 grants certain write privileges for templates, which allows remote authenticated administrators to execute arbitrary PHP code.	unknown 2008-07-25	6.0	CVE-2008-3298 BUGTRAQ XF
tuxplanet -- bilboblog	SQL injection vulnerability in admin/delete.php in BilboBlog 0.2.1, when magic_quotes_gpc is disabled, allows remote authenticated administrators to execute arbitrary SQL commands via the num parameter.	unknown 2008-07-25	6.0	CVE-2008-3302 MILW0RM XF
tuxplanet -- bilboblog	admin/login.php in BilboBlog 0.2.1, when register_globals is enabled, allows remote attackers to bypass authentication and obtain administrative access via a direct request that sets the login, admin_login, password, and admin_passwd parameters.	unknown 2008-07-25	6.8	CVE-2008-3303 MILW0RM BID XF
tuxplanet -- bilboblog	BilboBlog 0.2.1 allows remote attackers to obtain sensitive information via (1) an enable_cache=false query string to	unknown 2008-07-25	5.0	CVE-2008-3304 MILW0RM XF

	footer.php or (2) a direct request to pagination.php, which reveals the installation path in an error message.			
VIM Development Group -- VIM	src/configure.in in Vim 5.0 through 7.1, when used for a build with Python support, does not ensure that the Makefile-conf temporary file has the intended ownership and permissions, which allows local users to execute arbitrary code by writing to this file during a time window associated with a race condition.	unknown 2008-07-24	4.6	CVE-2008-3294 FULLDISC
winsoftmagic -- winremotepc_full winsoftmagic -- winremotepc_lite	WRPCServer.exe in WinSoftMagic WinRemotePC (WRPC) Lite 2008 and Full 2008 allows remote attackers to cause a denial of service (CPU consumption) via a crafted packet to TCP port 4321.	unknown 2008-07-24	5.0	CVE-2008-3269 MILW0RM BID
XOOPS -- Xoops	Cross-site scripting (XSS) vulnerability in modules/system/admin.php in XOOPS 2.0.18.1 allows remote attackers to inject arbitrary web script or HTML via the fct parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	4.3	CVE-2008-3295 BID XF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
OpenBSD -- OpenSSH OpenSSH -- OpenSSH	OpenSSH before 5.1 sets the SO_REUSEADDR socket option when the X11UseLocalhost configuration setting is disabled, which allows local users on some platforms to hijack the X11 forwarding port via a bind to a single IP address, as demonstrated on the HP-UX platform.	unknown 2008-07-22	1.2	CVE-2008-3259 OTHER-REF OTHER-REF BID
tuxplanet -- bilboblog	Multiple cross-site scripting (XSS) vulnerabilities in BilboBlog 0.2.1 allow remote authenticated administrators to inject arbitrary web script or HTML via the (1) content parameter to admin/update.php, related	unknown 2008-07-25	3.5	CVE-2008-3301 MILW0RM BID XF

	to conflicting code in widget.php; and allow remote attackers to inject arbitrary web script or HTML via the (2) titleId parameter to head.php, reachable through index.php; the (3) t_lang[lang_copyright] parameter to footer.php; the (4) content parameter to the default URI under admin/; the (5) url, (6) t_lang[lang_admin_help], (7) t_lang[lang_admin_clear_cache], (8) t_lang[lang_admin_home], and (9) t_lang[lang_admin_logout] parameters to admin/homelink.php; and the (10) t_lang[lang_admin_new_post] parameter to admin/post.php. NOTE: some of these details are obtained from third party information.	

Back to top