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
1024 CMS -- 1024 CMS	SQL injection vulnerability in includes/system.php in 1024 CMS 1.4.2 beta and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via a cookpass cookie.	unknown 2008-04-22	7.5	CVE-2008-1911 MILW0RM BID SECUNIA
5th_avenue_software -- 5th_avenue_shopping_cart	SQL injection vulnerability in store_pages/category_list.php in 5th Avenue Shopping Cart 1.2 trial edition allows remote attackers to execute arbitrary SQL commands via the category_ID parameter.	unknown 2008-04-23	7.5	CVE-2008-1921 BUGTRAQ MILW0RM OTHER-REF OTHER-REF BID SECUNIA XF
Adobe -- Photoshop	Buffer overflow in Adobe Photoshop Album Starter Edition 3.2, and possibly After Effects CS3, allows user-assisted remote attackers and physically proximate attackers to execute arbitrary	unknown 2008-04-23	9.3	CVE-2008-1765 FULLDISC MILW0RM OTHER-REF FRSIRT

	code via a BMP file with an invalid image header. NOTE: the related issue in Photoshop CS3 is already covered by CVE-2007-2244.			SECTRACK SECUNIA BID XF
Aspindir -- philboard	Multiple SQL injection vulnerabilities in W1L3D4 Philboard 1.0 allow remote attackers to execute arbitrary SQL commands via the (1) id and (2) topic parameters to (a) philboard_reply.asp, and the (3) forumid parameter to (b) philboard_newtopic.asp, different vectors than CVE-2007-2641 and CVE-2007-0920.	unknown 2008-04-25	7.5	CVE-2008-1939 MILW0RM BID XF
Asterisk -- s800i Asterisk -- Asterisk Business Edition Asterisk -- Asterisk Appliance Developer Kit Asterisk -- AsteriskNOW Asterisk -- Open Source	The IAX2 channel driver (chan_iax2) in Asterisk 1.2 before revision 72630 and 1.4 before revision 65679, when configured to allow unauthenticated calls, sends "early audio" to an unverified source IP address of a NEW message, which allows remote attackers to cause a denial of service (traffic amplification) via a spoofed NEW message.	unknown 2008-04-23	7.1	CVE-2008-1923 OTHER-REF OTHER-REF OTHER-REF
bigantsoft -- bigant_messenger	Stack-based buffer overflow in the AntServer module (AntServer.exe) in BigAnt IM Server in BigAnt Messenger 2.2 allows remote attackers to execute arbitrary code via a long URI in a request to TCP port 6080. NOTE: some of these details are obtained from third party information.	unknown 2008-04-22	10.0	CVE-2008-1914 MILW0RM BID SECUNIA XF
Borland -- Interbase	Stack-based buffer overflow in the database service (ibserver.exe) in Borland InterBase 2007 SP2 allows remote attackers to execute arbitrary code via a malformed opcode 0x52 request to TCP port 3050. NOTE: this might overlap CVE-2007-5243 or CVE-2007-5244.	unknown 2008-04-22	10.0	CVE-2008-1910 BUGTRAQ MILW0RM BID SECTRACK XF
Carbon Communities -- Carbon Communities	option_Update.asp in Carbon Communities 2.4 and earlier allows remote attackers to edit arbitrary member information via a modified ID field.	unknown 2008-04-22	7.5	CVE-2008-1900 BUGTRAQ
Chadha Software Technologies -- phpkb Knowledge Base	SQL injection vulnerability in comment.php in PHP Knowledge Base (PHPKB) 1.5 and 2.0 allows remote	unknown 2008-04-22	7.5	CVE-2008-1909 MILW0RM BID

	attackers to execute arbitrary SQL commands via the ID parameter.			SECUNIA XF
Cicoandcico -- CcMail	Cicoandcico CcMail 1.0.1 and earlier does not verify that the this_cookie cookie corresponds to an authenticated session, which allows remote attackers to obtain access to the "admin area" via a modified this_cookie cookie.	unknown 2008-04-22	7.5	CVE-2008-1904 MILW0RM BID SECUNIA
Classifieds Caffe -- Classifieds Caffe	SQL injection vulnerability in index.php in Classifieds Caffe allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in an add action. NOTE: this issue might be site-specific.	unknown 2008-04-25	7.5	CVE-2008-1936 BUGTRAQ MILW0RM BID FRSIRT
cpCommerce -- cpCommerce	Multiple SQL injection vulnerabilities in functions/display_page.func.php in cpCommerce 1.1.0 allow remote attackers to execute arbitrary SQL commands via the (1) id_product, (2) id_manufacturer, and (3) id_category parameters to unspecified components. NOTE: this probably overlaps CVE-2007-2959 and CVE-2007-2890.	unknown 2008-04-22	7.5	CVE-2008-1907 MILW0RM OTHER-REF BID
cpCommerce -- cpCommerce	Multiple directory traversal vulnerabilities in cpCommerce 1.1.0 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in (1) the language parameter in a language action to the default URI, which is not properly handled in actions/language.act.php, or (2) the action parameter to category.php.	unknown 2008-04-22	7.5	CVE-2008-1908 MILW0RM OTHER-REF BID FRSIRT
Crazy Goomba -- Crazy Goomba	SQL injection vulnerability in commentaires.php in Crazy Goomba 1.2.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-04-25	7.5	CVE-2008-1934 MILW0RM BID FRSIRT
Debian -- aptlinex	aptlinex before 0.91 allows local users to overwrite arbitrary files via a symlink attack on the gambas-apt.lock temporary file.	unknown 2008-04-22	7.2	CVE-2008-1901 OTHER-REF XF
DivX -- DivX Player	Stack-based buffer overflow in DivX Player 6.7 build 6.7.0.22 and earlier allows user-assisted remote attackers to cause a denial of service (application crash) or execute arbitrary code via a	unknown 2008-04-22	9.3	CVE-2008-1912 BUGTRAQ MILW0RM BID FRSIRT

	long subtitle in a .SRT file.			SECUNIA
ICQ -- Mirabilis ICQ	Heap-based buffer overflow in the boxelyRenderer module in the Personal Status Manager feature in ICQ 6.0 build 6043 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted personal status message.	unknown 2008-04-23	7.5	CVE-2008-1920 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Joomla -- Joomla	SQL injection vulnerability in the Filiale 1.0.4 component for Joomla! allows remote attackers to execute arbitrary SQL commands via the idFiliale parameter.	unknown 2008-04-25	7.5	CVE-2008-1935 MILW0RM BID FRSIRT
lasernet_cms -- lasernet_cms	SQL injection vulnerability in index.php in Lasernet CMS 1.5 and 1.11, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the new parameter in a new action.	unknown 2008-04-22	7.5	CVE-2008-1913 MILW0RM SECUNIA
Linux -- Util-linux	Argument injection vulnerability in login (login-utils/login.c) in util-linux-ng 2.14 and earlier makes it easier for remote attackers to hide activities by modifying portions of log events, as demonstrated by appending an "addr=" statement to the login name, aka "audit log injection."	unknown 2008-04-24	7.5	CVE-2008-1926 OTHER-REF OTHER-REF
Microsoft -- ie	Buffer overflow in the Microsoft HeartbeatCtl ActiveX control in HRTBEAT.OCX allows remote attackers to execute arbitrary code via the Host argument to an unspecified method.	unknown 2008-04-23	9.3	CVE-2007-6255 MS CERT-VN BID XF
newanz -- newsoffice	PHP remote file inclusion vulnerability in news_show.php in Newanz NewsOffice 1.0 and 1.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the newsoffice_directory parameter.	unknown 2008-04-22	7.5	CVE-2008-1903 MILW0RM BID SECUNIA XF
reddot -- cms	SQL injection vulnerability in ioRD.asp in RedDot CMS 7.5 Build 7.5.0.48, and possibly other versions including 6.5 and 7.0, allows remote attackers to execute arbitrary SQL commands via the LngId parameter.	unknown 2008-04-22	7.5	CVE-2008-1613 BUGTRAQ MILW0RM OTHER-REF BID

YourFreeWorld -- apartment_search_script	SQL injection vulnerability in listtest.php in YourFreeWorld Apartment Search Script allows remote attackers to execute arbitrary SQL commands via the r parameter.	unknown 2008-04-23	7.5	CVE-2008-1919 MILW0RM BID SECUNIA XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
amfphp -- amfphp	Multiple cross-site scripting (XSS) vulnerabilities in AMFPHP 1.2 allow remote attackers to inject arbitrary web script or HTML via the (1) class parameter to (a) methodTable.php, (b) code.php, and (c) details.php in browser/; and the (2) location parameter to browser/code.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-23	4.3	CVE-2008-1917 BID
Asterisk -- s800i Asterisk -- Asterisk Business Edition Asterisk -- Asterisk Appliance Developer Kit Asterisk -- AsteriskNOW Asterisk -- Open Source	The IAX2 channel driver (chan_iax2) in Asterisk Open Source 1.0.x, 1.2.x before 1.2.28, and 1.4.x before 1.4.19.1; Business Edition A.x.x, B.x.x before B.2.5.2, and C.x.x before C.1.8.1; AsteriskNOW before 1.0.3; Appliance Developer Kit 0.x.x; and s800i before 1.1.0.3, when configured to allow unauthenticated calls, does not verify that an ACK response contains a call number matching the server's reply to a NEW message, which allows remote attackers to cause a denial of service (traffic amplification) via a spoofed ACK response that does not complete a 3-way handshake. NOTE: this issue exists because of an incomplete fix for CVE-2008-1923.	unknown 2008-04-23	4.3	CVE-2008-1897 OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
Blender -- Blender	Stack-based buffer overflow in the imb_loadhdr function in Blender 2.45 allows user-assisted remote attackers to execute arbitrary code via a .blend file that contains a crafted Radiance RGBE image.	unknown 2008-04-22	6.8	CVE-2008-1102 OTHER-REF BID FRSIRT SECUNIA
cpCommerce -- cpCommerce	Cross-site scripting (XSS) vulnerability in calendar.php in cpCommerce 1.1.0 allows remote attackers to inject arbitrary web script or HTML via the year parameter in a view.year action.	unknown 2008-04-22	4.3	CVE-2008-1906 MILW0RM OTHER-REF BID FRSIRT

Debian -- aptlinex	The GUI for aptlinex before 0.91 does not sufficiently warn the user of potentially dangerous actions, which allows remote attackers to remove or modify packages via an apt:// URL.	unknown 2008-04-22	5.0	CVE-2008-1902 OTHER-REF XF
devworx -- blogworx	SQL injection vulnerability in view.asp in DevWorx BlogWorx 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-23	6.8	CVE-2008-1915 BID XF
Drupal -- Ubercart Module	Multiple cross-site scripting (XSS) vulnerabilities in the Ubercart 5.x before 5.x-1.0-rc1 module for Drupal allow remote attackers to inject arbitrary web script or HTML via text fields intended for the (1) address and (2) order information, which are later displayed on the order view page and unspecified other administrative pages, a different vulnerability than CVE-2008-1428.	unknown 2008-04-23	4.3	CVE-2008-1916 OTHER-REF FRSIRT XF
foxit_software -- reader	Foxit Reader 2.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a PDF file with (1) a malformed ExtGState resource containing a /Font resource, or (2) an XObject resource with a Rotate setting, which triggers memory corruption. NOTE: this is probably a different vulnerability than CVE-2007-2186.	unknown 2008-04-25	6.8	CVE-2008-1942 OTHER-REF OTHER-REF BID FRSIRT SECUNIA
GNU -- Emacs GNU -- sccs	vcdiff in Emacs 20.7 to 22.1.50, when used with SCCS, allows local users to overwrite arbitrary files via a symlink attack on temporary files.	unknown 2008-04-22	4.6	CVE-2008-1694 OTHER-REF OTHER-REF BID FRSIRT FRSIRT SECUNIA SECUNIA
grsecurity -- grsecurity Kernel Patch	The RBAC functionality in grsecurity before 2.1.11-2.6.24.5 and 2.1.11-2.4.36.2 does not enforce user_transition_deny and user_transition_allow rules for the (1) sys_setfsuid and (2) sys_setfsgid calls, which allows local users to bypass restrictions for those calls.	unknown 2008-04-25	4.6	CVE-2008-1940 OTHER-REF BID FRSIRT SECUNIA
Imager -- Imager	Buffer overflow in Imager 0.42 through 0.63 allows attackers to cause a denial of service (crash) via an image based fill in which the number of input channels is different from the	unknown 2008-04-24	5.0	CVE-2008-1928 OTHER-REF

	number of output channels.			
Inspire IRCd -- InspIRCd	Buffer overflow in InspIRCd before 1.1.18, when using the namesx and uhnames modules, allows remote attackers to cause a denial of service (daemon crash) via a large number of channel users with crafted nicknames, idents, and long hostnames.	unknown 2008-04-24	5.0	CVE-2008-1925 OTHER-REF OTHER-REF MLIST FRSIRT SECUNIA
Microsoft -- Zune Software	Absolute path traversal vulnerability in a certain ActiveX control in Zune allows user-assisted remote attackers to overwrite arbitrary files via the SaveToFile method. NOTE: the victim must explicitly allow the code to run.	2008-04-21 2008-04-25	4.3	CVE-2008-1933 BUGTRAQ MILW0RM
MoinMoin -- MoinMoin	The user form processing (userform.py) in MoinMoin before 1.6.3, when using ACLs or a non-empty superusers list, does not properly manage users, which allows remote attackers to gain privileges.	unknown 2008-04-25	6.8	CVE-2008-1937 OTHER-REF OTHER-REF BID FRSIRT SECUNIA XF
Nero -- Nero Nero -- MediaHome	NMMediaServer.exe in Nero MediaHome 3.3.3.0 and earlier, as used in Nero 8.3.2.1 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a long HTTP request to TCP port 54444, a different vector than CVE-2007-2322.	unknown 2008-04-22	5.0	CVE-2008-1905 OTHER-REF FRSIRT SECUNIA
Perl -- perl	Double free vulnerability in Perl 5.8.8 allows context-dependent attackers to cause a denial of service (memory corruption and crash) via a crafted regular expression containing UTF8 characters. NOTE: this issue might only be present on certain operating systems.	unknown 2008-04-24	5.0	CVE-2008-1927 OTHER-REF OTHER-REF
PHP_Fusion -- PHP_Fusion	SQL injection vulnerability in submit.php in PHP-Fusion 6.01.14 and 6.00.307, when magic_quotes_gpc is disabled and the database table prefix is known, allows remote authenticated users to execute arbitrary SQL commands via the submit_info[] parameter.	unknown 2008-04-23	6.0	CVE-2008-1918 MILW0RM OTHER-REF BID SECUNIA
phpMyAdmin -- phpMyAdmin	Unspecified vulnerability in phpMyAdmin before 2.11.5.2, when running on shared hosts, allows attackers with CREATE table permissions to read arbitrary files via a crafted HTTP POST request, related to use of an undefined UploadDir variable.	unknown 2008-04-23	4.3	CVE-2008-1924 OTHER-REF FRSIRT SECUNIA

Python Software Foundation -- Python	Multiple integer overflows in imageop.c in Python before 2.5.3 allow context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted images that trigger heap-based buffer overflows. NOTE: this issue is due to an incomplete fix for CVE-2007-4965.	unknown 2008-04-22	6.8	CVE-2008-1679 OTHER-REF OTHER-REF DEBIAN SECUNIA
Realtek -- HD Audio Codec Drivers	Realtek HD Audio Codec Drivers RTKVHDA.sys and RTKVHDA64.sys before 6.0.1.5605 on Windows Vista allow local users to create, write, and read registry keys via a crafted IOCTL request.	unknown 2008-04-25	6.8	CVE-2008-1931 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Realtek -- HD Audio Codec Drivers	Integer overflow in Realtek HD Audio Codec Drivers RTKVHDA.sys and RTKVHDA64.sys before 6.0.1.5605 on Windows Vista allows local users to execute arbitrary code via a crafted IOCTL request.	unknown 2008-04-25	6.8	CVE-2008-1932 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
S9Y -- Serendipity	Cross-site scripting (XSS) vulnerability in the Top Referrers (aka referrer) plugin in Serendipity (S9Y) before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via the Referer HTTP header.	unknown 2008-04-23	4.3	CVE-2008-1385 BUGTRAQ FULLDISC OTHER-REF OTHER-REF BID SECTRACK SECUNIA
S9Y -- Serendipity	Multiple cross-site scripting (XSS) vulnerabilities in the installer in Serendipity (S9Y) 1.3 allow remote attackers to inject arbitrary web script or HTML via (1) unspecified path fields or (2) the database host field. NOTE: the timing window for exploitation of this issue might be limited.	unknown 2008-04-23	4.3	CVE-2008-1386 BUGTRAQ FULLDISC OTHER-REF OTHER-REF BID SECTRACK
Sony -- mylo_com_2	Sony Mylo COM-2 Japanese model firmware before 1.002 does not properly verify web server SSL certificates, which allows remote attackers to obtain sensitive information and conduct spoofing attacks.	unknown 2008-04-25	5.0	CVE-2008-1938 OTHER-REF OTHER-REF SECUNIA
VideoLAN -- VLC	Multiple integer overflows in VLC before 0.8.6f allow remote attackers to cause a denial of service (crash) via the (1) MP4 demuxer, (2) Real demuxer, and (3) Cinepak codec, which triggers a buffer overflow.	unknown 2008-04-25	6.8	CVE-2008-1768 GENTOO
VideoLAN -- VLC	VLC before 0.8.6f allow remote attackers to cause a denial of service (crash) via a crafted	unknown 2008-04-25	6.8	CVE-2008-1769 OTHER-REF

	Cinepak file that triggers an out-of-bounds array access and memory corruption.		OTHER-REF GENTOO

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Akiva -- WebBoard	Cross-site scripting (XSS) vulnerability in the profile update feature in Akiva WebBoard 8.0 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors in the form field. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-04-25	3.5	CVE-2008-1941 BID SECUNIA

Back to top