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**
4xem -- vatctrl_class d-link -- mpeg4_shm_audio_control vivotek -- rtsp_mpeg4_sp_control	Stack-based buffer overflow in VATDecoder.VatCtrl.1 ActiveX control in (1) 4xem VatCtrl Class (VATDecoder.dll 1.0.0.27 and 1.0.0.51), (2) D-Link MPEG4 SHM Audio Control (VAPGDecoder.dll 1.7.0.5), (3) Vivotek RTSP MPEG4 SP Control (RtspVapgDecoderNew.dll 2.0.0.39), and possibly other products, allows remote attackers to execute arbitrary code via a long Url property. NOTE: some of these details are obtained from third party information.	2008-10-28	9.3	CVE-2008-4771 XF BID MILW0RM FRSIRT SECUNIA
adobe -- pagemaker	Stack-based buffer overflow in Adobe PageMaker 7.0.1 allows user-assisted remote attackers to execute arbitrary code via a .PMD file with a crafted font structure, a different vulnerability than CVE-2007-5169.	2008-10-30	9.3	CVE-2007-5394 BID
adobe -- pagemaker	Heap-based buffer overflow in Adobe PageMaker 7.0.1 allows user-assisted remote attackers to execute arbitrary code via a .PMD file with a crafted font structure.	2008-10-30	9.3	CVE-2007-6021 BID
aflog -- aflog	aflog 1.01 allows remote attackers to bypass authentication and gain administrative access by setting the aflog_auth_a cookie to "A" or "O" in (1) edit_delete.php, (2) edit_cat.php, (3) edit_lock.php, and (4) edit_form.php.	2008-10-29	7.5	CVE-2008-4784 XF BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
aiocp -- aiocp	SQL injection vulnerability in public/code/cp_polls_results.php in All In One Control Panel (AIOCP) 1.4 allows remote attackers to execute arbitrary SQL commands via the poll_id parameter.	2008-10-29	7.5	CVE-2008-4782 MILW0RM SECUNIA
aj_square_inc -- rss_reader	SQL injection vulnerability in EditUrl.php in AJ Square RSS Reader allows remote attackers to execute arbitrary SQL commands via the url parameter.	2008-10-27	7.5	CVE-2008-4753 XF BID MILW0RM
andrei_zmievski -- snoopy	The _httpsrequest function (Snoopy/Snoopy.class.php) in Snoopy 1.2.3 and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in https URLs. NOTE: some of these details are obtained from third party information.	2008-10-30	10.0	CVE-2008-4796 CONFIRM
db_soft_lab -- vimp_x	Multiple insecure method vulnerabilities in the VImpX.VImpAX ActiveX control (VImpX.ocx) 4.8.8.0 in DB Software Laboratory VImp X, possibly 4.7.7, allow remote attackers to overwrite arbitrary files via (1) the LogFile property and ClearLogFile method, and (2) the SaveToFile method.	2008-10-27	9.3	CVE-2008-4749 XF BID MILW0RM
dbsoftlab -- vimp_x	Stack-based buffer overflow in the VImpX.VImpAX ActiveX control (VImpX.ocx) 4.8.8.0 in DB Software Laboratory VImp X, possibly 4.7.7, allows remote attackers to execute arbitrary code via a long LogFile property.	2008-10-27	9.3	CVE-2008-4750 XF BID MILW0RM
dream4 -- koobi_cms	SQL injection vulnerability in the gallery module in Koobi CMS 4.3.0 allows remote attackers to execute arbitrary SQL commands via the galid parameter in a showimages action.	2008-10-29	7.5	CVE-2008-4778 BUGTRAQ MILW0RM
drupal -- drupal	The node module API in Drupal 5.x before 5.11 allows remote attackers to bypass node validation and have unspecified other impact via unknown vectors related to contributed modules.	2008-10-29	7.5	CVE-2008-4793 CONFIRM
e107 -- alternate_profiles_plugin	SQL injection vulnerability in newuser.php in the alternate_profiles plugin, possibly 0.2, for e107 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-29	7.5	CVE-2008-4785 BID MILW0RM
e107 -- easyshop_plugin	SQL injection vulnerability in easyshop.php in the EasyShop plugin for e107 allows remote attackers to execute arbitrary SQL commands via the category_id parameter.	2008-10-29	7.5	CVE-2008-4786 MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
easy-script -- myktools	Directory traversal vulnerability in update.php in MyKtools 2.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the langage parameter.	2008-10-29	7.5	CVE-2008-4781 BID MILW0RM
easy-script -- tlads	tlAds 1.0 allows remote attackers to bypass authentication and gain administrative access by setting the tlAds_login cookie to "admin."	2008-10-29	7.5	CVE-2008-4783 BID MILW0RM SECUNIA
freesshd -- freesshd	Stack-based buffer overflow in freeSSHd 1.2.1 allows remote authenticated users to cause a denial of service (service crash) and potentially execute arbitrary code via a long argument to the (1) rename and (2) realpath parameters.	2008-10-27	9.0	CVE-2008-4762 BID BUGTRAQ MILW0RM MILW0RM FRSIRT SECUNIA
ibm -- tivoli_storage_manager ibm -- tivoli_storage_manager_client ibm -- tivoli_storage_manager_express	Heap-based buffer overflow in the Data Protection for SQL CAD service (aka dsmcat.exe) in the Client Acceptor Daemon (CAD) and the scheduler in the Backup-Archive client 5.1.0.0 through 5.1.8.1, 5.2.0.0 through 5.2.5.2, 5.3.0.0 through 5.3.6.1, 5.4.0.0 through 5.4.2.2, and 5.5.0.0 through 5.5.0.91 in IBM Tivoli Storage Manager (TSM); and the Backup-Archive client in TSM Express; allows remote attackers to execute arbitrary code by sending a large amount of crafted data to a TCP port.	2008-10-30	10.0	CVE-2008-4801 XF MISC BID CONFIRM SECUNIA
joomla -- com_lms	SQL injection vulnerability in the Showroom Joomlearn LMS (com_lms) component for Joomla! and Mambo allows remote attackers to execute arbitrary SQL commands via the cat parameter in a showTests task.	2008-10-29	7.5	CVE-2008-4777 BID
kvirc -- kvirc	Format string vulnerability in the URI handler in KVirc 3.4.0, when set as the default application for processing IRC URIs, allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via format string specifiers in the irc:// URI.	2008-10-27	7.6	CVE-2008-4748 BID MILW0RM SECUNIA
o2php -- oxygen_bulletin_board	SQL injection vulnerability in member.php in Oxygen Bulletin Board 1.1.3 allows remote attackers to execute arbitrary SQL commands via the member parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-27	7.5	CVE-2008-4766 XF MISC BID

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
openoffice -- openoffice.org	Heap-based buffer overflow in OpenOffice.org (OOo) 2.x before 2.4.2 allows remote attackers to execute arbitrary code via a crafted WMF file associated with a StarOffice/StarSuite document.	2008-10-30	9.3	CVE-2008-2237 BID CONFIRM DEBIAN
openoffice -- openoffice.org	Heap-based buffer overflow in OpenOffice.org (OOo) 2.x before 2.4.2 allows remote attackers to execute arbitrary code via a crafted EMF file associated with a StarOffice/StarSuite document.	2008-10-30	9.3	CVE-2008-2238 BID CONFIRM DEBIAN
opera -- opera	Opera before 9.62 allows remote attackers to execute arbitrary commands via the History Search results page, a different vulnerability than CVE-2008-4696.	2008-10-30	9.3	CVE-2008-4794 XF BID CONFIRM
oscommerce -- poll_booth	SQL injection vulnerability in pollBooth.php in osCommerce Poll Booth Add-On 2.0 allows remote attackers to execute arbitrary SQL commands via the pollID parameter in a results operation. NOTE: this issue was disclosed by an unreliable researcher, so it might be incorrect.	2008-10-27	7.5	CVE-2008-4765 XF BID MISC
php-nuke -- downloadsplus_module	Unrestricted file upload vulnerability in the DownloadsPlus module in PHP-Nuke allows remote attackers to execute arbitrary code by uploading a file with (1) .htm, (2) .html, or (3) .txt extensions, then accessing it via a direct request to the file. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: it is unclear how allowing the upload of .html or .txt files supports arbitrary code execution; this might be legitimate functionality.	2008-10-28	9.0	CVE-2008-4767 XF BID MISC
phpdaily -- phpdaily	Multiple SQL injection vulnerabilities in PHP-Daily allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to (a) add_postit.php (b) delete.php, and (c) mod_prest_date.php; and the (2) prev parameter to (d) prest_detail.php.	2008-10-27	7.5	CVE-2008-4757 XF BID MILW0RM
pozscripts -- classified_auctions_script	SQL injection vulnerability in gotourl.php in PozScripts Classified Auctions Script allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-27	7.5	CVE-2008-4755 XF BID MILW0RM FRSIRT SECUNIA
questwork -- questcms	SQL injection vulnerability in main/main.php in QuestCMS allows remote attackers to execute arbitrary SQL commands via the obj	2008-10-28	7.5	CVE-2008-4772 BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	parameter.			
tech_logic -- tlnews	TlNews 2.2 allows remote attackers to bypass authentication and gain administrative access by setting the tlNews_login cookie to admin.	2008-10-27	7.5	CVE-2008-4752 XF BID MILW0RM SECUNIA
tguzip -- tguzip	Stack-based buffer overflow in TUGzip 3.5.0.0 allows remote attackers to denial of service (crash) or execute arbitrary code via a long filename in a .zip file.	2008-10-29	10.0	CVE-2008-4779 XF BID MILW0RM FRSIRT SECUNIA
tlm_cms -- tlm_cms	SQL injection vulnerability in TLM CMS 3.1 allows remote attackers to execute arbitrary SQL commands via the nom parameter to a-b-membres.php. NOTE: the goodies.php vector is already covered by CVE-2007-4808. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-10-28	7.5	CVE-2008-4768 XF MISC BID
webgui -- webgui	The loadModule function in lib/WebGUI/Asset.pm in WebGUI before 7.5.30 (stable) allows remote attackers to execute arbitrary code by uploading a Perl module and accessing it via a crafted URL.	2008-10-30	7.6	CVE-2008-4798 BID
wordpress -- wordpress	Directory traversal vulnerability in the get_category_template function in wp-includes/theme.php in WordPress 2.3.3 and earlier, and 2.5, allows remote attackers to include and possibly execute arbitrary PHP files via the cat parameter in index.php. NOTE: some of these details are obtained from third party information.	2008-10-28	9.3	CVE-2008-4769 BID MISC MISC SECUNIA

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
arihiro_kurta -- kantan_web_server	Directory traversal vulnerability in Arihiro Kurata Kantan WEB Server 1.8 and earlier allows remote attackers to read arbitrary files via unknown vectors.	2008-10-30	5.0	CVE-2008-4797 BID
buzzscripts -- buzzywall	Directory traversal vulnerability in download.php in BuzzyWall 1.3.1 allows remote attackers to read arbitrary local files via a .. (dot dot) in the id parameter.	2008-10-27	5.0	CVE-2008-4759 XF BID MILW0RM FRSIRT

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
drupal -- drupal	The validation functionality in the core upload module in Drupal 6.x before 6.5 allows remote authenticated users to bypass intended access restrictions and "attach files to content," related to a "logic error."	2008-10-29	6.0	CVE-2008-4789 CONFIRM
drupal -- drupal	The core upload module in Drupal 5.x before 5.11 allows remote authenticated users to bypass intended access restrictions and read "files attached to content" via unknown vectors.	2008-10-29	6.0	CVE-2008-4790 CONFIRM
drupal -- drupal	The user module in Drupal 5.x before 5.11 and 6.x before 6.5 might allow remote authenticated users to bypass intended login access rules and successfully login via unknown vectors.	2008-10-29	6.0	CVE-2008-4791 CONFIRM
drupal -- drupal	The core BlogAPI module in Drupal 5.x before 5.11 and 6.x before 6.5 does not properly validate unspecified content fields of an internal Drupal form, which allows remote authenticated users to bypass intended access restrictions via modified field values.	2008-10-29	6.0	CVE-2008-4792 CONFIRM
easy-script -- myforum	Directory traversal vulnerability in admin/centre.php in MyForum 1.3, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the padmin parameter.	2008-10-29	6.8	CVE-2008-4780 BID MILW0RM
epistream -- ipei_guestbook	Cross-site scripting (XSS) vulnerability in index.php in iPei Guestbook 2.0 allows remote attackers to inject arbitrary web script or HTML via the pg parameter, a different vector than CVE-2005-4597.	2008-10-27	4.3	CVE-2008-4751 XF BID BUGTRAQ FRSIRT SECUNIA MISC
graphiks -- myforum	SQL injection vulnerability in lecture.php in Graphiks MyForum 1.3, when register_globals is enabled, allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-10-27	6.8	CVE-2008-4760 XF BID MILW0RM FRSIRT
joomlacode -- extplorer	Directory traversal vulnerability in the eXtplorer module (com_extplorer) 2.0.0 RC2 and earlier in Joomla! allows remote attackers to read arbitrary files via a .. (dot dot) in the dir parameter in a show_error action.	2008-10-27	5.0	CVE-2008-4764 XF BID MILW0RM
kayako -- esupport	Cross-site scripting (XSS) vulnerability in includes/htmlArea/plugins/HtmlTidy/html-tidy-logic.php in Kayako eSupport 3.20.2 allows remote attackers to inject arbitrary web script or HTML via the jsMakeSrc parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: this issue is probably in the HTMLArea HTMLTidy (HTML Tidy) plugin, not eSupport.	2008-10-27	4.3	CVE-2008-4761 XF BID MLIST MISC

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
lynx -- lynx	Untrusted search path vulnerability in Lynx before 2.8.6rel.4 allows local users to execute arbitrary code via malicious (1) .mailcap and (2) mime.types files in the current working directory.	2008-10-27	4.6	CVE-2006-7234 CONFIRM SECTRACK BID REDHAT MLIST SECUNIA SECUNIA CONFIRM
microsoft -- internet_explorer	Visual truncation vulnerability in Microsoft Internet Explorer 6 allows remote attackers to spoof the address bar via a URL with a hostname containing many (Non-Blocking Space character) sequences, which are rendered as whitespace, aka MSRC ticket MSRC7899, a related issue to CVE-2003-1025.	2008-10-29	5.0	CVE-2008-4787 BID BUGTRAQ BUGTRAQ
microsoft -- internet_explorer	Microsoft Internet Explorer 6 omits high-bit URL-encoded characters when displaying the address bar, which allows remote attackers to spoof the address bar via a URL with a domain name that differs from an important domain name only in these characters, as demonstrated by using exam%A9ple.com to spoof example.com, aka MSRC ticket MSRC7900.	2008-10-29	5.0	CVE-2008-4788 BUGTRAQ BUGTRAQ
microsoft -- debug_diagnostic_tool	The DebugDiag ActiveX control in CrashHangExt.dll, possibly 1.0, in Microsoft Debug Diagnostic Tool allows remote attackers to cause a denial of service (NULL pointer dereference and Internet Explorer 6.0 crash) via a large negative integer argument to the GetEntryPointForThread method. NOTE: this issue might only be exploitable in limited environments or non-default browser settings.	2008-10-30	5.0	CVE-2008-4800 BID BUGTRAQ
netpbm -- netpbm	pamperspective in Netpbm before 10.35.48 does not properly calculate a window height, which allows context-dependent attackers to cause a denial of service (crash) via a crafted image file that triggers an out-of-bounds read.	2008-10-30	4.3	CVE-2008-4799 FEDORA FEDORA MLIST MLIST CONFIRM
opera -- opera	The links panel in Opera before 9.62 processes Javascript within the context of the "outermost page" of a frame, which allows remote attackers to inject arbitrary web script or HTML via cross-site scripting (XSS) attacks.	2008-10-30	4.3	CVE-2008-4795 BID
phpdaily -- phpdaily	Cross-site scripting (XSS) vulnerability in add_prest_date.php in PHP-Daily allows remote attackers to inject arbitrary web script or HTML via the date parameter.	2008-10-27	4.3	CVE-2008-4756 BID MILW0RM
phpdaily -- phpdaily	Directory traversal vulnerability in download_file.php in PHP-Daily allows remote attackers to read arbitrary local files via a .. (dot dot) in the fichier parameter.	2008-10-27	5.0	CVE-2008-4758 XF BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
				MILW0RM
questwork -- questcms	Directory traversal vulnerability in main/main.php in QuestCMS allows remote attackers to read arbitrary local files via a .. (dot dot) in the theme parameter.	2008-10-28	5.0	CVE-2008-4773 BID MILW0RM
questwork -- questcms	Cross-site scripting (XSS) vulnerability in main/main.php in QuestCMS allows remote attackers to inject arbitrary web script or HTML via the cx parameter.	2008-10-28	4.3	CVE-2008-4774 BID MILW0RM
scripts-for-sites -- ez_forum	SQL injection vulnerability in forum.php in Scripts for Sites (SFS) Ez Forum allows remote attackers to execute arbitrary SQL commands via the forum parameter.	2008-10-27	5.8	CVE-2008-4754 XF BID MILW0RM FRSIRT SECUNIA
wikidsystems -- wclient-php	Multiple cross-site scripting (XSS) vulnerabilities in sample.php in WiKID wClient-PHP 3.0-2 and earlier allow remote attackers to inject arbitrary web script or HTML via the PHP_SELF variable.	2008-10-27	4.3	CVE-2008-4763 BID
wojtek_kaniewsk -- libgadu	libgadu before 1.8.2 allows remote servers to cause a denial of service (crash) via a contact description with a large length, which triggers a buffer over-read.	2008-10-28	4.3	CVE-2008-4776 CONFIRM MLIST
Back to top				

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
phpmyadmin -- phpmyadmin	Cross-site scripting (XSS) vulnerability in pmd_pdf.php in phpMyAdmin 3.0.0, and possibly other versions including 2.11.9.2 and 3.0.1, when register_globals is enabled, allows remote attackers to inject arbitrary web script or HTML via the db parameter, a different vector than CVE-2006-6942 and CVE-2007-5977.	2008-10-28	2.6	CVE-2008-4775 BID BUGTRAQ SECUNIA
sun -- java_access_manager	Unspecified vulnerability in the search feature in Sun Java System LDAP JDK before 4.20 allows context-dependent attackers to obtain sensitive information via unknown attack vectors related to the LDAP JDK library.	2008-10-27	2.1	CVE-2008-4747 SUNALERT
Back to top				