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
21degrees -- symphony	SQL injection vulnerability in lib/class.admin.php in Twentyone Degrees Symphony 1.7.01 and earlier allows remote attackers to execute arbitrary SQL commands via the sym_auth cookie in a /publish/filemanager/ request to index.php.	unknown 2008-08-11	7.5	CVE-2008-3591 MILW0RM BID
21degrees -- symphony	Unrestricted file upload vulnerability in the File Manager in the admin panel in Twentyone Degrees Symphony 1.7.01 and earlier allows remote attackers to execute arbitrary code by uploading a file with an executable extension to a directory specified in the destination parameter, then accessing the uploaded file via a direct request, as demonstrated using workspace/masters/.	unknown 2008-08-11	8.5	CVE-2008-3592 MILW0RM
CA -- Internet Security Suite 2008 CA -- host_based_intrusion_prevention_system CA -- personal_firewall_2008 CA -- Internet Security Suite 2007 CA -- personal_firewall_2007	The kmxfw.sys driver in CA Host-Based Intrusion Prevention System (HIPS) r8, as used in CA Internet Security Suite and Personal Firewall, does not properly verify IOCTL requests, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted request.	unknown 2008-08-12	7.2	CVE-2008-2926 OTHER-REF BID

CalaCode -- atmail	Calacode @Mail 5.41 on Linux does not require administrative authentication for build-plesk-upgrade.php, which allows remote attackers to obtain sensitive information by creating and downloading a backup archive of the entire @Mail directory tree. NOTE: this can be leveraged for remote exploitation of CVE-2008-3395. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-10	7.8	CVE-2008-3579 XF
comsenz -- discuz	SQL injection vulnerability in index.php in Discuz! 6.0.1 allows remote attackers to execute arbitrary SQL commands via the searchid parameter in a search action.	unknown 2008-08-08	7.5	CVE-2008-3554 MILW0RM BID
Dayfox Designs -- dayfox_blog	Multiple directory traversal vulnerabilities in index.php in Dayfox Blog 4 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) p, (2) cat, and (3) archive parameters. NOTE: in some environments, this can be leveraged for remote file inclusion by using a UNC share pathname or an ftp, ftps, or ssh2.sftp URL.	unknown 2008-08-10	7.5	CVE-2008-3564 MILW0RM BID
Egi Zaberl -- e.z._poll	Multiple SQL injection vulnerabilities in admin/login.asp in E. Z. Poll 2 allow remote attackers to execute arbitrary SQL commands via the (1) Username and (2) Password parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-11	7.5	CVE-2008-3590 SECUNIA
GNU -- GnuTLS	Use after free vulnerability in the _gnutls_handshake_hash_buffers_clear function in lib/gnutls_handshake.c in libgnutls in GnuTLS 2.3.5 through 2.4.0 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via TLS transmission of data that is improperly used when the peer calls gnutls_handshake within a normal session, leading to attempted access to a deallocated libgcrypt handle.	unknown 2008-08-08	7.6	CVE-2008-2377 MLIST OTHER-REF OTHER-REF
Haudenschilt -- battlenet_clan_script	Multiple SQL injection vulnerabilities in index.php in Battle.net Clan Script 1.5.2 allow remote attackers to execute arbitrary SQL commands via the (1) showmember parameter in a members	unknown 2008-08-08	7.5	CVE-2008-3556 BUGTRAQ BID

	action and the (2) thread parameter in a board action. NOTE: vector 1 might be the same as CVE-2008-2522.			
Horde -- Groupware Webmail Edition	Multiple unspecified vulnerabilities in Horde Groupware Webmail before Edition 1.1.1 (final) have unknown impact and attack vectors related to "unescaped output," possibly cross-site scripting (XSS), in the (1) object browser and (2) contact view.	unknown 2008-08-12	9.0	CVE-2008-3650
HP -- HP-UX	Unspecified vulnerability in libc on HP HP-UX B.11.23 and B.11.31 allows remote attackers to cause a denial of service via unknown vectors.	unknown 2008-08-08	7.8	CVE-2008-1664 HP BID SECTRACK
HP -- HP-UX	Unspecified vulnerability in ftpd (aka wu-ftpd 2.4.x) in HP-UX B.11.11 allows remote attackers to gain privileges via unknown vectors.	unknown 2008-08-13	10.0	CVE-2008-1668 BID
HP -- Linux Imaging and Printing Project	The alert-mailing implementation in HP Linux Imaging and Printing (HPLIP) 1.6.7 allows local users to gain privileges and send e-mail messages from the root account via vectors related to the setalerts message, and lack of validation of the device URI associated with an event message.	unknown 2008-08-14	7.2	CVE-2008-2940 REDHAT SECTRACK
intellitamper -- intellitamper	Buffer overflow in the HTML parser in IntelliTamper 2.07 allows remote attackers to execute arbitrary code via a long URL in the SRC attribute of an IMG element. NOTE: this might be related to CVE-2008-3360.	unknown 2008-08-10	7.5	CVE-2008-3583 MILW0RM BID
IPsec-Tools -- racoon	src/racoon/handler.c in racoon in ipsec-tools does not remove an "orphaned ph1" (phase 1) handle when it has been initiated remotely, which allows remote attackers to cause a denial of service (resource consumption).	unknown 2008-08-12	7.8	CVE-2008-3652 MLIST
Joomla -- com_ezstore	SQL injection vulnerability in the EZ Store (com_ezstore) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a detail action to index.php.	unknown 2008-08-11	7.5	CVE-2008-3586 MILW0RM
Joomla -- com_user	components/com_user/models/reset.php in Joomla! 1.5 through 1.5.5 does not properly restrict access, which allows remote attackers to reset the "first enabled user (lowest id)" password, typically for the administrator.	unknown 2008-08-14	7.5	CVE-2008-3681 MILW0RM OTHER-REF BID SECTRACK

MagicScripts -- E-Store Kit-1 MagicScripts -- E-Store Kit-2	SQL injection vulnerability in viewdetails.php in MagicScripts E-Store Kit-1, E-Store Kit-2, E-Store Kit-1 Pro PayPal Edition, and E-Store Kit-2 PayPal Edition allows remote attackers to execute arbitrary SQL commands via the pid parameter.	unknown 2008-08-11	7.5	CVE-2008-3594 MILW0RM BID
Microsoft -- Windows Messenger	An ActiveX control (Messenger.UIAutomation.1) in Windows Messenger 4.7 and 5.1 is marked as safe-for-scripting, which allows remote attackers to "change state," obtain contact information, and establish audio or video connections without notification via unknown vectors.	unknown 2008-08-12	10.0	CVE-2008-0082 BID SECTRACK
Microsoft -- office_powerpoint_viewer	A "memory allocation error" in Microsoft PowerPoint Viewer 2003 allows remote attackers to execute arbitrary code via a PowerPoint file with a malformed picture index that triggers memory corruption, aka "Memory Allocation Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-0120
Microsoft -- office_powerpoint_viewer	A "memory calculation error" in Microsoft PowerPoint Viewer 2003 allows remote attackers to execute arbitrary code via a PowerPoint file with a malformed picture index that triggers memory corruption, aka "Memory Calculation Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-0121 MS
Microsoft -- Outlook Express Microsoft -- Windows Mail	The MHTML protocol handler in a component of Microsoft Outlook Express 5.5 SP2 and 6 through SP1, and Windows Mail, does not properly handle MHTML URL redirections, which allows remote attackers to bypass Internet Explorer domain restrictions via crafted HTTP headers, aka "URL Parsing Cross-Domain Information Disclosure Vulnerability."	unknown 2008-08-12	7.1	CVE-2008-1448 SECTRACK SECTRACK
Microsoft -- windows-nt	Array index vulnerability in the Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote authenticated users to execute arbitrary code via a crafted event subscription request that is used to access an array of function pointers.	unknown 2008-08-13	9.0	CVE-2008-1456
Microsoft -- windows-nt	The Event System in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 does not	unknown 2008-08-13	9.0	CVE-2008-1457 BID

	properly validate per-user subscriptions, which allows remote authenticated users to execute arbitrary code via a crafted event subscription request.			
Microsoft -- windows-nt	Heap-based buffer overflow in Microsoft Windows Image Color Management System (MSCMS) in the Image Color Management (ICM) component on Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP1 and SP2 allows remote attackers to execute arbitrary code via a crafted image file.	unknown 2008-08-12	9.3	CVE-2008-2245 SECTRACK
Microsoft -- windows-nt	Microsoft Windows Vista through SP1 and Server 2008 do not properly import the default IPsec policy from a Windows Server 2003 domain to a Windows Server 2008 domain, which prevents IPsec rules from being enforced and allows remote attackers to bypass intended access restrictions.	unknown 2008-08-12	7.8	CVE-2008-2246 SECTRACK
Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01, 6, and 7 accesses uninitialized memory, which allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, aka "HTML Object Memory Corruption Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2254 SECTRACK
Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01, 6, and 7 accesses uninitialized memory, which allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, a different vulnerability than CVE-2008-2254, aka "HTML Object Memory Corruption Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2255 SECTRACK
Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01, 6, and 7 does not properly handle objects that have been incorrectly initialized or deleted, which allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, aka "Uninitialized Memory Corruption Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2256 SECTRACK
Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01, 6, and 7 accesses uninitialized memory in certain conditions, which allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, a different vulnerability than CVE-2008-2258, aka "HTML Objects Memory Corruption Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2257 SECTRACK

Microsoft -- Internet Explorer	Microsoft Internet Explorer 5.01, 6, and 7 accesses uninitialized memory in certain conditions, which allows remote attackers to cause a denial of service (crash) and execute arbitrary code via unknown vectors, a different vulnerability than CVE-2008-2257, aka "HTML Objects Memory Corruption Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2258 SECTRACK
Microsoft -- Internet Explorer	Microsoft Internet Explorer 6 and 7 does not perform proper "argument validation" during print preview, which allows remote attackers to execute arbitrary code via unknown vectors, aka "HTML Component Handling Vulnerability."	unknown 2008-08-13	9.3	CVE-2008-2259 SECTRACK
Microsoft -- Office Microsoft -- office_excel_viewer	Microsoft Office Excel 2000 SP3, 2002 SP3, and 2003 SP2 and SP3; Office Excel Viewer 2003; and Office 2004 and 2008 for Mac do not properly validate index values when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Indexing Validation Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3004
Microsoft -- Office	Microsoft Office Excel 2000 SP3 and 2002 SP3, and Office 2004 and 2008 for Mac, do not properly validate an unspecified array index when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Index Array Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3005
Microsoft -- Office Microsoft -- SharePoint Server Microsoft -- office_compatibility_pack Microsoft -- office_excel_viewer	Microsoft Office Excel 2000 SP3, 2002 SP3, 2003 SP2 and SP3, and 2007 Gold and SP1; Office Excel Viewer 2003 Gold and SP3; Office Excel Viewer; Office Compatibility Pack 2007 Gold and SP1; Office SharePoint Server 2007 Gold and SP1; and Office 2004 and 2008 for Mac do not properly parse record values when loading Excel files, which allows remote attackers to execute arbitrary code via a crafted Excel file, aka the "Excel Record Parsing Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3006
Microsoft -- office_converter_pack Microsoft -- Office Microsoft -- Works	Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of a PICT file, which allows remote attackers to execute arbitrary code via a crafted PICT file, aka the "Malformed PICT Filter Vulnerability,"	unknown 2008-08-12	9.3	CVE-2008-3018 MS

	a different vulnerability than CVE-2008-3021.			
Microsoft -- office_converter_pack Microsoft -- Office Microsoft -- Works	Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of an Encapsulated PostScript (EPS) file, which allows remote attackers to execute arbitrary code via a crafted EPS file, aka the "Malformed EPS Filter Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3019
Microsoft -- office_converter_pack Microsoft -- Office Microsoft -- Works	Microsoft Office 2000 SP3 and XP SP3; Office Converter Pack; and Works 8 do not properly parse the length of a BMP file, which allows remote attackers to execute arbitrary code via a crafted BMP file, aka the "Malformed BMP Filter Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3020
Microsoft -- office_converter_pack Microsoft -- Office Microsoft -- Works	Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of a PICT file, which allows remote attackers to execute arbitrary code via a crafted PICT file, aka the "PICT Filter Parsing Vulnerability," a different vulnerability than CVE-2008-3018.	unknown 2008-08-12	9.3	CVE-2008-3021
Microsoft -- office_converter_pack Microsoft -- Office Microsoft -- Works	Microsoft Office 2000 SP3, XP SP3, and 2003 SP2; Office Converter Pack; and Works 8 do not properly parse the length of a WordPerfect Graphics (WPG) file, which allows remote attackers to execute arbitrary code via a crafted WPG file, aka the "WPG Image File Heap Corruption Vulnerability."	unknown 2008-08-12	9.3	CVE-2008-3460 MS
Microsoft -- windows-nt	nslookup.exe in Microsoft Windows XP SP2 allows user-assisted remote attackers to execute arbitrary code, as demonstrated by an attempted DNS zone transfer, and as exploited in the wild in August 2008.	unknown 2008-08-12	9.3	CVE-2008-3648 OTHER-REF BID
openimpro -- openimpro	SQL injection vulnerability in image.php in OpenImpro 1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-12	7.5	CVE-2008-3599 MILW0RM
PHP -- PHP	Buffer overflow in the imageloadfont function in ext/gd/gd.c in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.	unknown 2008-08-14	7.5	CVE-2008-3658 OTHER-REF OTHER-REF OTHER-REF MLIST MLIST

phsBlog -- phsBlog	Multiple SQL injection vulnerabilities in phsBlog 0.1.1 allow remote attackers to execute arbitrary SQL commands via the (1) eid parameter to comments.php, (2) cid parameter to index.php, and the (3) urltitle parameter to entries.php.	unknown 2008-08-11	7.5	CVE-2008-3588 MILW0RM
pozscripts -- greencart_php_shopping_cart	Multiple SQL injection vulnerabilities in PozScripts GreenCart PHP Shopping Cart allow remote attackers to execute arbitrary SQL commands via the id parameter to (1) product_desc.php and (2) store_info.php.	unknown 2008-08-11	7.5	CVE-2008-3585 MILW0RM BID
pozscripts -- classified_ads	SQL injection vulnerability in showcategory.php in PozScripts Classified Ads allows remote attackers to execute arbitrary SQL commands via the cid parameter, a different vector than CVE-2008-????. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-13	7.5	CVE-2008-3672
pozscripts -- classified_ads	SQL injection vulnerability in browsecats.php in PozScripts Classified Ads allows remote attackers to execute arbitrary SQL commands via the cid parameter, a different vector than CVE-2008-????.	unknown 2008-08-13	7.5	CVE-2008-3673 MILW0RM BID
pozscripts -- tubeguru_video_sharing_script	SQL injection vulnerability in ugroups.php in PozScripts TubeGuru Video Sharing Script allows remote attackers to execute arbitrary SQL commands via the UID parameter.	unknown 2008-08-13	7.5	CVE-2008-3674 MILW0RM BID
psi-labs -- psipuss	Multiple SQL injection vulnerabilities in psipuss 1.0 allow remote attackers to execute arbitrary SQL commands via (1) the Cid parameter to categories.php or (2) the Username parameter to login.php.	unknown 2008-08-12	7.5	CVE-2008-3598 MILW0RM BID
psychdaily -- php_ring_webring_system	admin/wr_admin.php in PHP-Ring Webring System (aka uPHP_ring_website) 0.9.1 allows remote attackers to bypass authentication and gain administrative access by setting the admin cookie to 1.	unknown 2008-08-12	7.5	CVE-2008-3602 MILW0RM BID
Quicksilver Forums -- Quicksilver Forums	SQL injection vulnerability in index.php in Quicksilver Forums 1.4.1 allows remote attackers to execute arbitrary SQL commands via the forums array parameter in a search action.	unknown 2008-08-12	7.5	CVE-2008-3601 MILW0RM BID
ruby-lang -- Ruby	Algorithmic complexity vulnerability in WEBrick::HTTP::DefaultFileHandler	unknown 2008-08-12	7.8	CVE-2008-3656 OTHER-REF

	in WEBrick in Ruby 1.8.5 and earlier, 1.8.5 through 1.8.6-p286, 1.8.7 through 1.8.7-p71, and 1.9 through r18423 allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted HTTP request that is processed by a backtracking regular expression.			OTHER-REF
ruby-lang -- Ruby	The dl module in Ruby 1.8.5 and earlier, 1.8.5 through 1.8.6-p286, 1.8.7 through 1.8.7-p71, and 1.9 through r18423 does not check "taintness" of inputs, which allows context-dependent attackers to bypass safe levels and execute dangerous functions by accessing a library using DL.dlopen.	unknown 2008-08-12	7.5	CVE-2008-3657 OTHER-REF OTHER-REF
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in snoop on Sun Solaris 8 through 10 and OpenSolaris before snv_96, when the -o option is omitted, allows remote attackers to execute arbitrary code via a crafted SMB packet, a different vulnerability than CVE-2008-0965.	unknown 2008-08-08	10.0	CVE-2008-0964 SUNALERT BID XF
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in snoop on Sun Solaris 8 through 10 and OpenSolaris before snv_96, when the -o option is omitted, allows remote attackers to execute arbitrary code via a crafted SMB packet, a different vulnerability than CVE-2008-0964.	unknown 2008-08-08	10.0	CVE-2008-0965 SUNALERT BID XF
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in Sun Solaris 10 and OpenSolaris before snv_96 allows (1) context-dependent attackers to cause a denial of service (panic) via vectors involving creation of a crafted file and use of the sendfilev system call, as demonstrated by a file served by an Apache 2.2.x web server with EnableSendFile configured; and (2) local users to cause a denial of service (panic) via a call to sendfilev or sendfile.	unknown 2008-08-13	7.1	CVE-2008-3666 SUNALERT BID
syzygycms -- syzygycms	Directory traversal vulnerability in index.php in SyzygyCMS 0.3 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.	unknown 2008-08-11	7.5	CVE-2008-3593 MILW0RM
Tibco -- Runtime Agent Tibco -- mainframe_service_tracker Tibco -- Hawk Tibco -- iprocess_engine	Multiple buffer overflows in TIBCO Hawk (1) AMI C library (libtibhawkami) and (2) Hawk HMA (tibhawkhma), as used in TIBCO Hawk before 4.8.1; Runtime Agent (TRA) before 5.6.0; iProcess Engine 10.3.0	unknown 2008-08-13	10.0	CVE-2008-3338 OTHER-REF

	through 10.6.2 and 11.0.0; and Mainframe Service Tracker before 1.1.0 might allow remote attackers to execute arbitrary code via a crafted message.			
TikiWiki -- tikiki_cms_groupware	Multiple unspecified vulnerabilities in TikiWiki CMS/Groupware before 2.0 have unknown impact and attack vectors.	unknown 2008-08-12	10.0	CVE-2008-3653 OTHER-REF
TikiWiki -- tikiki_cms_groupware	Unspecified vulnerability in TikiWiki CMS/Groupware before 2.0 allows attackers to obtain "path and PHP configuration" via unknown vectors.	unknown 2008-08-12	7.8	CVE-2008-3654 OTHER-REF OTHER-REF
txtsql -- txtsql	PHP remote file inclusion vulnerability in examples/txtSQLAdmin/startup.php in txtSQL 2.2 Final allows remote attackers to execute arbitrary PHP code via a URL in the CFG[txtsql][class] parameter.	unknown 2008-08-12	9.3	CVE-2008-3595 MILW0RM BID
Vacation Rentals -- Vacation Rental Script	SQL injection vulnerability in index.php in Vacation Rental Script 3.0 allows remote attackers to execute arbitrary SQL commands via the id parameter in a sections action.	unknown 2008-08-12	7.5	CVE-2008-3603 MILW0RM BID
Xerox -- phaser	The Xerox Phaser 8400 allows remote attackers to cause a denial of service (reboot) via an empty UDP packet to port 1900.	unknown 2008-08-10	7.8	CVE-2008-3571 MILW0RM BID
zeescripts -- zeebuddy	SQL injection vulnerability in bannerclick.php in ZeeBuddy 2.1 allows remote attackers to execute arbitrary SQL commands via the adid parameter.	unknown 2008-08-12	7.5	CVE-2008-3604 MILW0RM BID XF
zeescripts -- zeereviews	SQL injection vulnerability in comments.php in ZeeScripts Reviews Opinions Rating Posting Engine Web-Site PHP Script (aka ZeeReviews) allows remote attackers to execute arbitrary SQL commands via the ItemID parameter.	unknown 2008-08-13	7.5	CVE-2008-3669 MILW0RM BID XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Acronis -- true_image_echo_server	Acronis True Image Echo Server 9.x build 8072 on Linux does not properly encrypt backups to an FTP server, which allows remote attackers to obtain sensitive information. NOTE: the provenance	unknown 2008-08-13	5.0	CVE-2008-3671 BID

	of this information is unknown; the details are obtained solely from third party information.			
Adobe -- presenter	Multiple cross-site scripting (XSS) vulnerabilities in files generated by Adobe Presenter 6 and 7 before 7.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors involving (1) viewer.swf and (2) loadflash.js, a different vulnerability than CVE-2008-3516.	unknown 2008-08-12	4.3	CVE-2008-3515
Adobe -- presenter	Multiple cross-site scripting (XSS) vulnerabilities in files generated by Adobe Presenter 6 and 7 before 7.0.1 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors involving (1) viewer.swf and (2) loadflash.js, a different vulnerability than CVE-2008-3515.	unknown 2008-08-12	4.3	CVE-2008-3516
Apache Friends -- XAMPP	Multiple cross-site scripting (XSS) vulnerabilities in XAMPP 1.6.7, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the text parameter to (1) iart.php and (2) ming.php.	unknown 2008-08-10	4.3	CVE-2008-3569 BUGTRAQ BID
Apache Software Foundation -- Tomcat	Directory traversal vulnerability in Apache Tomcat 6.0.0 through 6.0.16, when allowLinking and UTF-8 are enabled, allows remote attackers to read arbitrary files via encoded directory traversal sequences in the URI, a different vulnerability than CVE-2008-2370.	unknown 2008-08-12	4.3	CVE-2008-2938 MILW0RM BID
articlefriendly -- article_friendly	SQL injection vulnerability in categorydetail.php in Article Friendly Standard allows remote attackers to execute arbitrary SQL commands via the Cat parameter.	unknown 2008-08-12	6.8	CVE-2008-3649 MILW0RM BID
articlefriendly -- article_friendly	SQL injection vulnerability in authordetail.php in Article Friendly Pro allows remote attackers to execute arbitrary SQL commands via the autid parameter.	unknown 2008-08-13	6.8	CVE-2008-3670 MILW0RM BID
Computer Associates -- Internet Security Suite Computer Associates -- personal_firewall Computer Associates -- host_based_intrusion_prevention_system	Unspecified vulnerability in the kmxfw.sys driver in CA Host-Based Intrusion Prevention System (HIPS) r8, as used in CA Internet Security Suite and Personal Firewall, allows remote attackers to cause a denial of service via unknown vectors, related	unknown 2008-08-12	5.0	CVE-2008-3174 OTHER-REF BID

	to "insufficient validation."			
Damian Hickey -- freeway	Cross-site scripting (XSS) vulnerability in admin/search_links.php in Freeway before 1.4.2.197 allows remote attackers to inject arbitrary web script or HTML via the URL.	unknown 2008-08-14	4.3	CVE-2008-3678 OTHER-REF
Flagship Industries -- Ventrilo	The decryption function in Flagship Industries Ventrilo 3.0.2 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) by sending a type 0 packet with an invalid version followed by another packet to TCP port 3784.	unknown 2008-08-14	5.0	CVE-2008-3680 BUGTRAQ OTHER-REF OTHER-REF BID
gelatocms -- gelatocms	Directory traversal vulnerability in classes/imgsize.php in Gelato 0.95 allows remote attackers to read arbitrary files via (1) a .. (dot dot) and possibly (2) full pathname in the img parameter. NOTE: some of these details are obtained from third party information.	unknown 2008-08-14	5.0	CVE-2008-3675 MILW0RM
harmoni -- harmoni	Cross-site scripting (XSS) vulnerability in Harmoni before 1.4.7 allows remote attackers to inject arbitrary web script or HTML via the Username field, which is inserted into logs that could be rendered when viewed by an administrator.	unknown 2008-08-12	4.3	CVE-2008-3596 OTHER-REF BID
havp -- havp havp -- http_antivirus_proxy	sockethandler.cpp in HTTP Antivirus Proxy (HAVP) 0.88 allows remote attackers to cause a denial of service (hang) by connecting to a non-responsive server, which triggers an infinite loop due to an uninitialized variable.	unknown 2008-08-14	4.3	CVE-2008-3688 OTHER-REF
hMailServer -- hMailServer	Unspecified vulnerability in the IMAP server in hMailServer 4.4.1 allows remote authenticated users to cause a denial of service (resource exhaustion or daemon crash) via a long series of IMAP commands.	unknown 2008-08-14	4.3	CVE-2008-3676 BUGTRAQ
HP -- Linux Imaging and Printing Project	The hpssd message parser in hpssd.py in HP Linux Imaging and Printing (HPLIP) 1.6.7 allows local users to cause a denial of service (process stop) via a crafted packet, as demonstrated by sending "msg=0" to TCP port 2207.	unknown 2008-08-14	4.9	CVE-2008-2941 REDHAT SECTRACK

iDevspot -- PhpLinkExchange	Multiple cross-site scripting (XSS) vulnerabilities in index.php in IDevSpot PhpLinkExchange 1.01 allow remote attackers to inject arbitrary web script or HTML via the catid parameter in a (1) user_add, (2) recip, (3) tellafriend, or (4) contact action, or (5) in a request without an action; or (6) the id parameter in a tellafriend action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-08-14	4.3	CVE-2008-3679 OTHER-REF BID XF
Linux -- Kernel	The (1) real_lookup and (2) __lookup_hash functions in fs/namei.c in the vfs implementation in the Linux kernel before 2.6.25.15 does not prevent creation of a child dentry for a deleted (aka S_DEAD) directory, which allows local users to cause a denial of service ("overflow" of the UBIFS orphan area) via a series of attempted file creations within deleted directories.	unknown 2008-08-12	4.9	CVE-2008-3275 MLIST OTHER-REF OTHER-REF OTHER-REF BID
Linux -- ipsec_tools_racoon_daemon	Memory leak in racoon/proposal.c in the racoon daemon in ipsec-tools before 0.7.1 allows remote authenticated users to cause a denial of service (memory consumption) via invalid proposals.	unknown 2008-08-12	4.0	CVE-2008-3651 MLIST OTHER-REF
Linux -- Kernel	The rt6_fill_node function in Linux kernel 2.6.26-rc4, 2.6.26.2, and possibly other 2.6.26 versions, allows local users to cause a denial of service (kernel OOPS) via IPv6 requests when no IPv6 input device is in use, which triggers a NULL pointer dereference.	unknown 2008-08-14	4.9	CVE-2008-3686 MLIST MLIST
Marcello Brandao -- yogurt_social_network_module	Multiple cross-site scripting (XSS) vulnerabilities in the Yogurt Social Network module 3.2 rc1 for XOOPS allow remote attackers to inject arbitrary web script or HTML via the uid parameter to (1) friends.php, (2) seutubo.php, (3) album.php, (4) scrapbook.php, (5) index.php, or (6) tribes.php; or (7) the description field of a new scrap.	unknown 2008-08-13	4.3	CVE-2008-3668 OTHER-REF BID BID XF XF
Maxthon -- maxthon_browser	Stack-based buffer overflow in Maxthon Browser 2.0 and earlier allows remote attackers to execute arbitrary code via a long Content-type HTTP header.	unknown 2008-08-13	6.8	CVE-2008-3667 OTHER-REF BID XF

McAfee -- encrypted_usb_manager	Unspecified vulnerability in McAfee Encrypted USB Manager 3.1.0.0, when the Re-use Threshold for passwords is nonzero, allows remote attackers to conduct offline brute force attacks via unknown vectors.	unknown 2008-08-12	6.8	CVE-2008-3605
Menalto -- Gallery	Directory traversal vulnerability in contrib/phpBB2/modules.php in Gallery 1.5.7 and 1.6-alpha3, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the phpEx parameter within a modload action.	unknown 2008-08-12	6.8	CVE-2008-3600 BUGTRAQ MILW0RM OTHER-REF
Microsoft -- office_powerpoint Microsoft -- office_powerpoint_viewer Microsoft -- Office Microsoft -- compatibility_pack_word_excel_powerpoint	A "memory calculation error" in Microsoft Office PowerPoint 2000 SP3, 2002 SP3, 2003 SP2, and 2007 through SP1; Office Compatibility Pack for Word, Excel, and PowerPoint 2007 through SP1; and Office 2004 for Mac allows remote attackers to execute arbitrary code via a PowerPoint file with crafted list values that trigger memory corruption, aka "Parsing Overflow Vulnerability."	unknown 2008-08-12	6.8	CVE-2008-1455
Microsoft -- Office	Microsoft Office Excel 2007 Gold and SP1, does not properly delete the PWD (password) string from connections.xml when a .xlsx file is configured not to save the remote data session password, which allows local users to obtain sensitive information and obtain access to a remote data source, aka the "Excel Credential Caching Vulnerability."	unknown 2008-08-12	6.6	CVE-2008-3003
mozilo -- mozilocms	Directory traversal vulnerability in download.php in moziloCMS 1.10.1, when magic_quotes_gpc is disabled, allows remote attackers to read arbitrary files via a .. (dot dot) in the cat parameter.	unknown 2008-08-11	4.3	CVE-2008-3589 MILW0RM BID
needscripts -- homes_4_sale	Cross-site scripting (XSS) vulnerability in result.php in Chris Bunting Homes 4 Sale allows remote attackers to inject arbitrary web script or HTML via the r parameter.	unknown 2008-08-11	4.3	CVE-2008-3587 BUGTRAQ BID
noticeware -- email_server	The IMAP server in NoticeWare Email Server NG 4.6.3 and earlier allows remote attackers to cause a denial of service (daemon crash) via	unknown 2008-08-12	5.0	CVE-2008-3607 BUGTRAQ BID

	multiple long LOGIN commands.			
openfreeway -- Freeway	Directory traversal vulnerability in includes/events_application_top.php in Freeway before 1.4.2.197 allows remote attackers to include and execute arbitrary local files via unspecified vectors.	unknown 2008-08-14	6.8	CVE-2008-3677 OTHER-REF
OpenTTD -- OpenTTD	Buffer overflow in src/openttd.cpp in OpenTTD before 0.6.2 allows local users to execute arbitrary code via a large filename supplied to the "-g" parameter in the ttd_main function. NOTE: it is unlikely that this issue would cross privilege boundaries in typical environments.	unknown 2008-08-10	4.6	CVE-2008-3577 OTHER-REF BID
PHP -- PHP	Buffer overflow in the memnstr function in PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via the delimiter argument to the explode function. NOTE: the scope of this issue is limited since most applications would not use an attacker-controlled delimiter, but local attacks against safe_mode are feasible.	unknown 2008-08-14	6.4	CVE-2008-3659 OTHER-REF OTHER-REF MLIST MLIST MLIST MLIST
PHP -- PHP	PHP 4.4.x before 4.4.9 and PHP 5.6 through 5.2.6, when used as a FastCGI module, allows remote attackers to cause a denial of service (crash) via a request with multiple dots preceding the extension, as demonstrated using foo..php.	unknown 2008-08-14	5.0	CVE-2008-3660 OTHER-REF MLIST MLIST
Pidgin -- Pidgin	The NSS plugin in libpurple in Pidgin 2.4.3 does not verify SSL certificates, which makes it easier for remote attackers to trick a user into accepting an invalid server certificate for a spoofed service.	unknown 2008-08-08	6.8	CVE-2008-3532 OTHER-REF OTHER-REF OTHER-REF
Powergap -- shopsystem	SQL injection vulnerability in s03.php in Powergap Shopsystem, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the ag parameter.	unknown 2008-08-10	6.8	CVE-2008-3561 OTHER-REF BID
Qbik -- WinGate	Heap-based buffer overflow in the IMAP service in Qbik WinGate 6.2.2.1137 and earlier allows remote authenticated users to cause a denial of service (resource exhaustion) or possibly execute arbitrary code via a	unknown 2008-08-12	6.5	CVE-2008-3606 BUGTRAQ BID SECTRACK

	long argument to the LIST command. NOTE: some of these details are obtained from third party information.			
Red Hat -- Network Satellite Server	manzier.pxt in Red Hat Network Satellite Server before 5.1.1 has a hard-coded authentication key, which allows remote attackers to connect to the server and obtain sensitive information about user accounts and entitlements.	unknown 2008-08-14	6.4	CVE-2008-2369 REDHAT BID SECTRACK
ruby-lang -- Ruby	The regular expression engine (regex.c) in Ruby 1.8.5 and earlier, 1.8.6 through 1.8.6-p286, 1.8.7 through 1.8.7-p71, and 1.9 through r18423 allows remote attackers to cause a denial of service (infinite loop and crash) via multiple long requests to a Ruby socket, related to memory allocation failure, and as demonstrated against Webrick.	unknown 2008-08-14	5.0	CVE-2008-3443 MILW0RM
ruby-lang -- Ruby	Ruby 1.8.5 and earlier, 1.8.5 through 1.8.6-p286, 1.8.7 through 1.8.7-p71, and 1.9 through r18423 does not properly restrict access to critical variables and methods at various safe levels, which allows context-dependent attackers to bypass intended access restrictions via (1) untrace_var (2) $PROGRAM_NAME, and (3) syslog at safe level 4, and (4) insecure methods at safe levels 1 through 3.	unknown 2008-08-12	6.4	CVE-2008-3655 OTHER-REF OTHER-REF
Skulltag Team -- Skulltag	Skulltag before 0.97d2-RC6 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) by sending a "command 29" packet when the player is not in the game.	unknown 2008-08-12	5.0	CVE-2008-3597 OTHER-REF XF
Sun -- Java System Web Proxy Server	Unspecified vulnerability in the FTP subsystem in Sun Java System Web Proxy Server 4.0 through 4.0.5 before SP6 allows remote attackers to cause a denial of service (failure to accept connections) via unknown vectors, probably related to exhaustion of file descriptors.	unknown 2008-08-14	5.0	CVE-2008-3683
VMWare -- VirtualCenter	Unspecified vulnerability in VMware VirtualCenter 2.5 before Update 2 and 2.0.2 before Update 5 allows attackers to determine valid user names via an "attempt to assign	unknown 2008-08-13	5.0	CVE-2008-3514 BUGTRAQ BID

	permissions to other system users."			
Xen -- Xen Xen -- xen_flask_module	Heap-based buffer overflow in the flask_security_label function in Xen 3.3, when compiled with the XSM:FLASK module, allows unprivileged domain users (domU) to execute arbitrary code via the flask_op hypercall.	unknown 2008-08-14	6.8	CVE-2008-3687 OTHER-REF OTHER-REF
ypninc -- php_realty	SQL injection vulnerability in dpage.php in YPN PHP Realty allows remote attackers to execute arbitrary SQL commands via the docID parameter.	unknown 2008-08-14	6.8	CVE-2008-3682 OTHER-REF BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
amaroK -- Amarok	The MagnatuneBrowser::listDownloadComplete function in magnatunebrowser/magnatunebrowser.cpp in Amarok before 1.4.10 allows local users to overwrite arbitrary files via a symlink attack on the album_info.xml temporary file.	unknown 2008-08-14	1.9	CVE-2008-3699 OTHER-REF OTHER-REF OTHER-REF
Pluck -- Pluck	Multiple cross-site scripting (XSS) vulnerabilities in Pluck 4.5.2, when register_globals is enabled, allow remote attackers to inject arbitrary web script or HTML via the (1) lang_footer parameter to (a) data/inc/footer.php; the (2) pluck_version, (3) lang_install22, (4) titelkop, (5) lang_kop1, (6) lang_kop2, (7) lang_modules, (8) lang_kop4, (9) lang_kop15, (10) lang_kop5, and (11) titelkop parameters to (b) data/inc/header.php; the pluck_version and titelkop parameters to (c) data/inc/header2.php; and the (14) lang_theme6 parameter to (d) data/inc/themeinstall.php.	unknown 2008-08-10	2.6	CVE-2008-3574 BUGTRAQ

Back to top