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
Cisco	Cisco Unified Communications Manager 4.1 before 4.1(3)SR7, 4.2 before 4.2(3)SR4, 4.3 before 4.3(2), 5.x before 5.1(3), and 6.x before 6.1(1) does not properly validate SIP URLs, which allows remote attackers to cause a denial of service (service interruption) via a SIP INVITE message, aka Bug ID CSCsl22355.	unknown 2008-05-16	7.8	CVE-2008-1748 BID FRSIRT SECTRACK XF
ALAXALA -- AX_router	Unspecified vulnerability in AlaxalA AX routers allows remote attackers to cause a denial of service (dropped session) via crafted BGP UPDATE messages, leading to route flapping, possibly a related issue to CVE-2007-6372.	unknown 2008-05-13	7.1	CVE-2008-2171 OTHER-REF CERT-VN BID
arubanetworks -- ArubaOS	Unspecified vulnerability in the TACACS authentication component in Aruba Mobility Controller 3.1.x, 3.2.x, and 3.3.x allows remote authenticated users to gain privileges via unknown vectors.	unknown 2008-05-16	9.0	CVE-2008-2273 OTHER-REF
buyscripts -- vshare_you_tube_clone	SQL injection vulnerability in group_posts.php in vShare YouTube Clone 2.6 allows remote attackers to execute arbitrary SQL commands via the tid parameter.	unknown 2008-05-14	7.5	CVE-2008-2223 MILW0RM
castle_rock -- SNMPc	Stack-based buffer overflow in the Network Manager in Castle Rock Computing SNMPc 7.1 and earlier allows remote attackers to cause a denial of service (crash) or execute	unknown 2008-05-14	7.5	CVE-2008-2214 BID SECTRACK XF

	arbitrary code via a long community string in an SNMP TRAP packet.			
Century Software -- router	Unspecified vulnerability in Century routers allows remote attackers to cause a denial of service (dropped session) via crafted BGP UPDATE messages, leading to route flapping, possibly a related issue to CVE-2007-6372.	unknown 2008-05-13	7.1	CVE-2008-2170 CERT-VN BID
Cisco -- Unified Presence Cisco -- Unified Presence Server	The Presence Engine (PE) service in Cisco Unified Presence before 6.0(1) allows remote attackers to cause a denial of service (core dump and service interruption) via malformed packets, aka Bug ID CSCsh50164.	unknown 2008-05-16	7.8	CVE-2008-1158 CISCO BID SECTRACK XF
Cisco -- Unified Presence	The Presence Engine (PE) service in Cisco Unified Presence before 6.0(1) allows remote attackers to cause a denial of service (core dump and service interruption) via an unspecified "stress test," aka Bug ID CSCsh20972.	unknown 2008-05-16	7.8	CVE-2008-1740 BID SECTRACK XF
Cisco -- Unified Presence	The SIP Proxy (SIPD) service in Cisco Unified Presence before 6.0(3) allows remote attackers to cause a denial of service (core dump and service interruption) via a TCP port scan, aka Bug ID CSCsj64533.	unknown 2008-05-16	7.8	CVE-2008-1741 BID SECTRACK XF
Cisco -- Unified Communications Manager Cisco -- Unified CallManager	The Certificate Authority Proxy Function (CAPF) service in Cisco Unified Communications Manager (CUCM) 4.1 before 4.1(3)SR7, 4.2 before 4.2(3)SR4, and 4.3 before 4.3(2) allows remote attackers to cause a denial of service (service crash) via malformed network traffic, aka Bug ID CSCsk46770.	unknown 2008-05-16	7.8	CVE-2008-1744 CISCO BID SECTRACK XF
Cisco -- Unified Communications Manager Cisco -- Unified CallManager	Unspecified vulnerability in Cisco Unified Communications Manager 4.1 before 4.1(3)SR6, 4.2 before 4.2(3)SR3, 4.3 before 4.3(2), 5.x before 5.1(3), and 6.x before 6.1(1) allows remote attackers to cause a denial of service (CCM service restart) via an unspecified SIP INVITE message, aka Bug ID CSCsk46944.	unknown 2008-05-16	7.8	CVE-2008-1747 CISCO BID SECTRACK XF
Cisco -- cisco_content_switching_module Cisco -- cisco_content_switching_module_SSL	Memory leak in Cisco Content Switching Module (CSM) 4.2(3) up to 4.2(8) and Cisco Content Switching Module with SSL (CSM-S) 2.1(2) up to 2.1(7) allows remote attackers to cause a denial of service (memory consumption) via TCP segments with an unspecified combination of TCP flags.	unknown 2008-05-14	7.8	CVE-2008-1749

DeluxeBB -- DeluxeBB	SQL injection vulnerability in forums.php in DeluxeBB 1.2 and earlier allows remote attackers to execute arbitrary SQL commands via the sort parameter.	unknown 2008-05-14	7.5	CVE-2008-2194 MILW0RM BID
Drumster -- blogme_php	SQL injection vulnerability in comments.php in Gamma Scripts BlogMe PHP 1.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-13	7.5	CVE-2008-2175 MILW0RM BID
Drupal -- Drupal Drupal -- Site_Documentation_Module	The Site Documentation Drupal module 5.x before 5.x-1.8 and 6.x before 6.x-1.1 allows remote authenticated users to gain privileges of other users by leveraging the "access content" permission to list tables and obtain session IDs from the database.	unknown 2008-05-16	9.3	CVE-2008-2271 OTHER-REF
Emophp -- EMO Realty Manager	SQL injection vulnerability in news.php in EMO Realty Manager allows remote attackers to execute arbitrary SQL commands via the ida parameter.	unknown 2008-05-16	7.5	CVE-2008-2265 MILW0RM BID
EQdkp -- EQdkp	SQL injection vulnerability in login.php in EQdkp 1.3.2f allows remote attackers to bypass EQdkp user authentication via the user_id parameter.	unknown 2008-05-14	7.5	CVE-2008-2222 MILW0RM BID
freelanceauction.eu -- Freelance Auction Script	SQL injection vulnerability in browseproject.php in Freelance Auction Script 1.0 allows remote attackers to execute arbitrary SQL commands via the pid parameter in a pdetails action.	unknown 2008-05-16	7.5	CVE-2008-2278 MILW0RM BID XF
gamecms -- gamecms_lite	SQL injection vulnerability in index.php in gameCMS Lite 1.0 allows remote attackers to execute arbitrary SQL commands via the systemId parameter.	unknown 2008-05-14	7.5	CVE-2008-2225 MILW0RM BID XF
Hitachi -- GR4000 Hitachi -- GR3000 Hitachi -- GR2000 Avici -- router	Unspecified vulnerability in Avici routers allows remote attackers to cause a denial of service (dropped session) via crafted BGP UPDATE messages, leading to route flapping, possibly a related issue to CVE-2007-6372.	unknown 2008-05-13	7.1	CVE-2008-2169 CERT-VN BID
Hitachi -- GR2000 Hitachi -- GR3000 Hitachi -- GR4000	Unspecified vulnerability in Hitachi GR routers allows remote attackers to cause a denial of service (dropped session) via crafted BGP UPDATE messages, leading to route flapping, possibly a related issue to CVE-2007-6372.	unknown 2008-05-13	7.1	CVE-2008-2172 OTHER-REF CERT-VN BID
IBM -- WebSphere Application Server	Unspecified vulnerability in the Java plugin in IBM WebSphere Application Server 5.0.2 allows untrusted applets to gain privileges	unknown 2008-05-14	7.5	CVE-2008-2221 AIXAPAR BID

	via unknown attack vectors.			
Interact -- Interact	Multiple PHP remote file inclusion vulnerabilities in Interact Learning Community Environment Interact 2.4.1, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) CONFIG[LANGUAGE_CPATH] parameter to modules/forum/embedforum.php and the (2) CONFIG[BASE_PATH] parameter to modules/scorm/lib.inc.php, different vectors than CVE-2006-4448.	unknown 2008-05-14	7.5	CVE-2008-2220 MILW0RM BID XF
ITCMS -- ITCMS	Static code injection vulnerability in box/minichat/boxpop.php in IT!CMS (aka itcms) 1.9 allows remote attackers to inject arbitrary PHP code into box/MiniChat/data/shouts.php via the shout parameter.	unknown 2008-05-14	7.5	CVE-2008-2192 MILW0RM BID XF
Kalptaru Infotech -- Feedback and Rating Script	SQL injection vulnerability in detail.php in Feedback and Rating Script 1.0 allows remote attackers to execute arbitrary SQL commands via the listingid parameter.	unknown 2008-05-16	7.5	CVE-2008-2277 MILW0RM BID XF
Kevin Ludlow -- AustinSmoke GasTracker	AustinSmoke GasTracker (AS-GasTracker) 1.0.0 allows remote attackers to bypass authentication and gain privileges by setting the gastracker_admin cookie to TRUE.	unknown 2008-05-16	7.5	CVE-2008-2269 MILW0RM BID
Links_Pile -- Automated Link Exchange Portal	SQL injection vulnerability in linking.page.php in Automated Link Exchange Portal allows remote attackers to execute arbitrary SQL commands via the cat_id parameter. NOTE: linking.page.php is commonly renamed to link.php, links.php, etc.	unknown 2008-05-16	7.5	CVE-2008-2263 MILW0RM BID
Linux -- Kernel	Memory leak in the ipip6_rcv function in net/ipv6/sit.c in the Linux kernel before 2.6.25.3 allows remote attackers to cause a denial of service (memory consumption) via network traffic to a Simple Internet Transition (SIT) tunnel interface, related to the pskb_may_pull and kfree_skb functions, and management of an skb reference count.	unknown 2008-05-16	7.8	CVE-2008-2136 MLIST OTHER-REF BID XF
maian_script_world -- maian_search	SQL injection vulnerability in search.php in Maian Search 1.1 allows remote attackers to execute arbitrary SQL commands via the keywords parameter in a search action.	unknown 2008-05-14	7.5	CVE-2008-2203 BUGTRAQ BID XF

maian_script_world -- maian_music	SQL injection vulnerability in index.php in Maian Music 1.1 allows remote attackers to execute arbitrary SQL commands via the album parameter in an album action.	unknown 2008-05-14	7.5	CVE-2008-2205 BUGTRAQ BID XF
maianscriptworld -- maian_greeting	SQL injection vulnerability in index.php in Maian Greeting 2.1 allows remote attackers to execute arbitrary SQL commands via the keywords parameter in a search action.	unknown 2008-05-14	7.5	CVE-2008-2208 BUGTRAQ BID XF
Mantis -- Mantis	Cross-site request forgery (CSRF) vulnerability in Mantis 1.1.1 allows remote attackers to create new administrative users via user_create.	unknown 2008-05-16	9.3	CVE-2008-2276 OTHER-REF SECUNIA
Microsoft -- Office	Unspecified vulnerability in Microsoft Publisher in Office 2000 and XP SP3, 2003 SP2 and SP3, and 2007 SP1 and earlier allows remote attackers to execute arbitrary code via a Publisher file with crafted object header data that triggers memory corruption, aka "Publisher Object Handler Validation Vulnerability."	unknown 2008-05-13	8.5	CVE-2008-0119 BID SECTRACK
Microsoft -- windows-nt	The I2O Utility Filter driver (i2omgmt.sys) 5.1.2600.2180 for Microsoft Windows XP sets Everyone/Write permissions for the "\\.\I2OExc" device interface, which allows local users to gain privileges. NOTE: this issue can be leveraged to overwrite arbitrary memory and execute code via an IOCTL call with a crafted DeviceObject pointer.	unknown 2008-05-13	7.2	CVE-2008-0322
Microsoft -- Office_compatibility_pack_for_word_excel_ppt_2007 Microsoft -- Office Microsoft -- word_viewer	Unspecified vulnerability in Microsoft Word in Office 2000 and XP SP3, 2003 SP2 and SP3, and 2007 Office System SP1 and earlier allows remote attackers to execute arbitrary code via a Rich Text Format (.rtf) file with a malformed string that triggers a "memory calculation error" and a heap-based buffer overflow, aka "Object Parsing Vulnerability."	unknown 2008-05-13	9.3	CVE-2008-1091 CERT-VN
Microsoft -- Office_compatibility_pack_for_word_excel_ppt_2007 Microsoft -- Office Microsoft -- word_viewer	Unspecified vulnerability in Microsoft Word in Office 2000 and XP SP3, 2003 SP2 and SP3, and 2007 Office System SP1 and earlier allows remote attackers to execute arbitrary code via a Word file with a malformed Cascading Style Sheet (CSS) value, related to a "memory handling error" that triggers memory corruption.	unknown 2008-05-13	9.3	CVE-2008-1434

Microsoft -- windows_ce	Multiple unspecified vulnerabilities in the JPEG (GDI+) and GIF image processing in Microsoft Windows CE 5.0 allow remote attackers to execute arbitrary code via crafted JPEG and GIF images.	unknown 2008-05-12	9.3	CVE-2008-2160 MSKB BID
miniweb2 -- miniweb	SQL injection vulnerability in the blogwriter module 2.0 for Miniweb allows remote attackers to execute arbitrary SQL commands via the historymonth parameter to index.php.	unknown 2008-05-14	7.5	CVE-2008-2197 MILW0RM BID
PHP-Fusion -- PHP-Fusion	Multiple directory traversal vulnerabilities in PHP-Fusion Forum Rank System 6 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the settings[locale] parameter to (1) forum.php and (2) profile.php in infusions/rank_system/. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-14	7.5	CVE-2008-2227 OTHER-REF BID XF
PHPWAY -- Kostenloses_Linkmanagementscript	Multiple PHP remote file inclusion vulnerabilities in PHPWAY Kostenloses Linkmanagementscript allow remote attackers to execute arbitrary PHP code via a URL in the (1) main_page_directory and (2) page_to_include parameters in template\index.php.	unknown 2008-05-16	7.5	CVE-2008-2270 MILW0RM BID
rdesktop -- rdesktop	Integer signedness error in the xrealloc function (rdesktop.c) in RDesktop 1.5.0 allows remote attackers to execute arbitrary code via unknown parameters, which triggers a heap-based overflow. NOTE: the role of the channel_process function was not specified by the original researcher.	unknown 2008-05-12	9.3	CVE-2008-1803 IDEFENSE OTHER-REF DEBIAN BID SECTRACK XF
romedchim_international_srl -- online_rent_property_script	SQL injection vulnerability in index.php in Online Rent (aka Online Rental Property Script) 4.5 and earlier allows remote attackers to execute arbitrary SQL commands via the pid parameter.	unknown 2008-05-14	7.5	CVE-2008-2190 BUGTRAQ MILW0RM BID XF
Sarg -- Squid Analysis Report Generator	Multiple stack-based buffer overflows in Sarg might allow attackers to execute arbitrary code via unknown vectors, probably a crafted Squid log file.	unknown 2008-05-13	7.5	CVE-2008-1922 SUSE
scorpnews -- scorpnews	PHP remote file inclusion vulnerability in example.php in Thomas Gossmann ScorpNews 2.0 allows remote attackers to execute arbitrary PHP code via a URL in the site parameter.	unknown 2008-05-14	7.5	CVE-2008-2193 MILW0RM BID

Sun -- Solaris	Multiple unspecified vulnerabilities in Solaris print service for Sun Solaris 8, 9, and 10 allow remote attackers to cause a denial of service or execute arbitrary code via unknown vectors.	unknown 2008-05-12	10.0	CVE-2008-2144 SUNALERT BID
tftp -- TFTP Server SP	Buffer overflow in TFTP Server SP 1.4 and 1.5 on Windows, and possibly other versions, allows remote attackers to execute arbitrary code via a long TFTP error packet. NOTE: some of these details are obtained from third party information.	unknown 2008-05-12	10.0	CVE-2008-2161 MILW0RM BID XF
toocharger -- smartblog	SQL injection vulnerability in index.php in SMartBlog (aka SMBlog) 1.3 allows remote attackers to execute arbitrary SQL commands via the idt parameter.	unknown 2008-05-13	7.5	CVE-2008-2183 MILW0RM BID
toocharger -- smartblog	Multiple SQL injection vulnerabilities in SMartBlog (aka SMBlog) 1.3 allow remote attackers to execute arbitrary SQL commands via the (1) mois, (2) an, (3) jour, and (4) id parameters to index.php, and the (5) login parameter to gestion/logon.php, different vectors than CVE-2008-2183. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-13	7.5	CVE-2008-2184
TYPO3 -- sr_feuser_register Extension	Unspecified vulnerability in sr_feuser_register 1.4.0, 1.6.0, 2.2.1 to 2.2.7, 2.3.0 to 2.3.6, 2.4.0, and 2.5.0 to 2.5.9 extension for TYPO3 allows remote attackers to execute arbitrary code and delete arbitrary files via unspecified attack vectors.	unknown 2008-05-16	7.5	CVE-2008-2275
Wordnet -- Wordnet	Stack-based buffer overflow in the searchwn function in Wordnet 2.0, 2.1, and 3.0 might allow context-dependent attackers to execute arbitrary code via a long command line option. NOTE: this issue probably does not cross privilege boundaries except in cases in which Wordnet is used as a back end.	unknown 2008-05-12	7.5	CVE-2008-2149 OTHER-REF
WordPress -- WordPress	wp-includes/vars.php in Wordpress before 2.2.3 does not properly extract the current pafe from the PATH_INFO ($PHP_SELF), which allows remote attackers to bypass intended access restrictions for certain pages.	unknown 2008-05-12	7.5	CVE-2008-2146 OTHER-REF OTHER-REF

xensource -- xen	Buffer overflow in the backend of XenSource Xen Para Virtualized Frame Buffer (PVFB) 3.0 through 3.1.2 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a crafted shared framebuffer.	unknown 2008-05-14	7.2	CVE-2008-1943 OTHER-REF BID SECTRACK
xensource -- xen	Buffer overflow in the backend framebuffer of XenSource Xen Para-Virtualized Framebuffer (PVFB) Message 3.0 through 3.0.3 allows local users to cause a denial of service (SDL crash) and possibly execute arbitrary code via "bogus screen updates."	unknown 2008-05-14	7.2	CVE-2008-1944 OTHER-REF BID SECTRACK
Xiph.Org -- libvorbis	Xiph.org libvorbis 1.2.0 and earlier does not properly handle a zero value for codebook.dim, which allows remote attackers to cause a denial of service (crash or infinite loop) or trigger an integer overflow.	unknown 2008-05-16	7.1	CVE-2008-1419 OTHER-REF XF XF
Yamaha -- router	Unspecified vulnerability in Yamaha routers allows remote attackers to cause a denial of service (dropped session) via crafted BGP UPDATE messages, leading to route flapping, possibly a related issue to CVE-2007-6372.	unknown 2008-05-13	7.1	CVE-2008-2173 CERT-VN BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
anserv -- auction_xl	SQL injection vulnerability in viewfaqs.php in AnServ Auction XL allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-05-14	6.8	CVE-2008-2189 BUGTRAQ MILW0RM BID XF
Apache Software Foundation -- Apache HTTP Server	Cross-site scripting (XSS) vulnerability Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.	unknown 2008-05-13	4.3	CVE-2008-2168 BUGTRAQ BUGTRAQ BUGTRAQ BID XF
arubanetworks -- aruba_mobility_controller	Mltiple cross-site scripting (XSS) vulnerabilities in the web interface in "Aruba Mobility Controller 2.4.8.x-FIPS, 2.5.5.x, 2.5.6.x, 3.1.1.x, 3.2.0.x, and 3.3.1.x allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-05-16	4.3	CVE-2008-2272 OTHER-REF
C-News.fr -- C-News	Cross-site scripting (XSS) vulnerability in install.php in C-News.fr C-News 1.0.1 allows remote attackers to inject arbitrary web script or HTML via the etape parameter.	unknown 2008-05-14	4.3	CVE-2008-2219 OTHER-REF BID

cilekyazilim -- chicomas	Cross-site scripting (XSS) vulnerability in index.php in Chilek Content Management System (aka ChiCoMaS) 2.0.4 allows remote attackers to inject arbitrary web script or HTML via the q parameter.	unknown 2008-05-13	4.3	CVE-2008-2186 BUGTRAQ BID XF
Cisco -- Unified Communications Manager	Memory leak in the Certificate Trust List (CTL) Provider service in Cisco Unified Communications Manager (CUCM) 5.x before 5.1(3) allows remote attackers to cause a denial of service (memory consumption and service interruption) via a series of malformed TCP packets, as demonstrated by TCPFUZZ, aka Bug ID CSCsj80609.	unknown 2008-05-16	4.3	CVE-2008-1742 CISCO BID SECTRACK XF
Cisco -- Unified Communications Manager	Memory leak in the Certificate Trust List (CTL) Provider service in Cisco Unified Communications Manager (CUCM) 5.x before 5.1(3) and 6.x before 6.1(1) allows remote attackers to cause a denial of service (memory consumption and service interruption) via a series of malformed TCP packets, aka Bug ID CSCsi98433.	unknown 2008-05-16	4.3	CVE-2008-1743 CISCO BID SECTRACK XF
Cisco -- Unified Communications Manager	Cisco Unified Communications Manager (CUCM) 5.x before 5.1(2) and 6.x before 6.1(1) allows remote attackers to cause a denial of service (service interruption) via a SIP JOIN message with a malformed header, aka Bug ID CSCsi48115.	unknown 2008-05-16	4.3	CVE-2008-1745 CISCO BID SECTRACK XF
Cisco -- Unified Communications Manager	The SNMP Trap Agent service in Cisco Unified Communications Manager (CUCM) 4.1 before 4.1(3)SR6, 4.2 before 4.2(3)SR3, 4.3 before 4.3(2), 5.x before 5.1(3), and 6.x before 6.1(1) allows remote attackers to cause a denial of service (core dump and service restart) via a series of malformed UDP packets, as demonstrated by the IP Stack Integrity Checker (ISIC), aka Bug ID CSCsj24113.	unknown 2008-05-16	4.3	CVE-2008-1746 CISCO BID SECTRACK XF
Cisco -- Building Broadband Service Manager	Cross-site scripting (XSS) vulnerability in AccessCodeStart.asp in Cisco Building Broadband Service Manager (BBSM) Captive Portal 5.3 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	unknown 2008-05-16	4.3	CVE-2008-2165 BUGTRAQ BUGTRAQ BID SECTRACK XF
CMS Made Simple -- CMS Made Simple	Incomplete blacklist vulnerability in javaUpload.php in Postlet in the FileManager module in CMS Made Simple 1.2.4 and earlier allows remote attackers to execute arbitrary code by uploading a file with a name ending in (1) .jsp, (2) .php3, (3) .cgi, (4) .dhtml, (5) .phtml, (6) .php5, or (7) .jar, then accessing it via a direct request to the file in modules/FileManager/postlet/.	unknown 2008-05-16	4.3	CVE-2008-2267 MILW0RM OTHER-REF VIM BID XF
cplinks -- cplinks	Multiple SQL injection vulnerabilities in cpLinks 1.03, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) admin_username parameter (aka the username field) to admin/index.php and the (2) search_text and (3) search_category parameters to search.php. NOTE: some of these details are obtained from third party information.	unknown 2008-05-13	6.8	CVE-2008-2180 MILW0RM
cplinks -- cplinks	Multiple cross-site scripting (XSS) vulnerabilities in search.php in cpLinks 1.03 allow remote attackers to inject arbitrary web script or HTML via	unknown 2008-05-13	4.3	CVE-2008-2181 MILW0RM

	the (1) search_text and (2) search_category parameters. NOTE: the XSS reportedly occurs in a forced SQL error message. NOTE: some of these details are obtained from third party information.			
Cyberfolio -- Cyberfolio	PHP remote file inclusion vulnerability in portfolio/commentaires/derniers_commentaires.php in Cyberfolio 7.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the rep parameter.	unknown 2008-05-14	6.8	CVE-2008-2228 MILW0RM
CyrixMED -- CyrixMED	Cross-site scripting (XSS) vulnerability in index.php in CyrixMED 1.4 allows remote attackers to inject arbitrary web script or HTML via the msg_erreur parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-16	4.3	CVE-2008-2264 BID XF
DeluxeBB -- DeluxeBB	Static code injection vulnerability in admincp.php in DeluxeBB 1.2 and earlier allows remote authenticated administrators to inject arbitrary PHP code into logs/cp.php via the URI.	unknown 2008-05-14	6.5	CVE-2008-2195 MILW0RM BID
eejj33 -- blackbook	Multiple cross-site scripting (XSS) vulnerabilities in EJ3 BlackBook 1.0 allow remote attackers to inject arbitrary web script or HTML via the (1) bookCopyright and (2) ver parameters to (a) footer.php, and the (3) bookName, (4) bookMetaTags, and (5) estiloCSS parameters to (b) header.php.	unknown 2008-05-13	4.3	CVE-2008-2188 BUGTRAQ BID XF
GNU -- XEmacs GNU -- Emacs	Emacs 21 and XEmacs automatically load and execute .flc (fast lock) files that are associated with other files are edited within Emacs, which allows user-assisted attackers to execute arbitrary code.	unknown 2008-05-12	6.8	CVE-2008-2142 OTHER-REF OTHER-REF OTHER-REF
HP -- HP-UX	Unspecified vulnerability in the FTP server for HP-UX B.11.11, B.11.23, and B.11.31 allows remote authenticated users to cause a denial of service (FTP server outage) via unknown attack vectors.	unknown 2008-05-13	6.8	CVE-2008-0713
IBM -- Lotus Quickr	Cross-site scripting (XSS) vulnerability in IBM Lotus Quickr 8.1 before Hotfix 5 for Windows and AIX, and before Hotfix 3 for i5/OS, allows remote attackers to inject arbitrary web script or HTML via unknown vectors related to "WYSIWYG editors."	unknown 2008-05-13	4.3	CVE-2008-2163 BID
Ilient -- SysAid	Cross-site scripting (XSS) vulnerability in SystemList.jsp in SysAid 5.1.08 allows remote attackers to inject arbitrary web script or HTML via the searchField parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-13	4.3	CVE-2008-2179
kkeim -- kmita_mail	PHP remote file inclusion vulnerability in kmitaadmin/kmitam/htmlcode.php in Kmita Mail 3.0 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the file parameter.	unknown 2008-05-14	6.8	CVE-2008-2199 BUGTRAQ MILW0RM BID XF
kmita_tellfriend -- tellfriend	PHP remote file inclusion vulnerability in kmitaadmin/kmitat/htmlcode.php in Kmita Tellfriend 2.0 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the file parameter.	unknown 2008-05-14	6.8	CVE-2008-2198 BUGTRAQ MILW0RM BID XF

LifeType -- LifeType	Cross-site scripting (XSS) vulnerability in admin.php in LifeType 1.2.7 allows remote attackers to inject arbitrary web script or HTML via the searchTerms parameter in an editArticleCategories operation (aka an admin category search).	unknown 2008-05-13	4.3	CVE-2008-2178 BUGTRAQ XF
LifeType -- LifeType	Cross-site scripting (XSS) vulnerability in admin.php in LifeType 1.2.8 allows remote attackers to inject arbitrary web script or HTML via the newBlogUserName parameter in an addBlogUser action, a different vector than CVE-2008-2178.	unknown 2008-05-14	4.3	CVE-2008-2196 BUGTRAQ BID
maian_script_world -- maian_weblog	Multiple cross-site scripting (XSS) vulnerabilities in Maian Weblog 4.0 allow remote attackers to inject arbitrary web script or HTML via the (1) keywords parameter to admin/index.php in a blogs search action, the (2) msg_charset and (3) msg_header9 parameters to admin/inc/header.php, and the (4) keywords parameter to index.php in a search action.	unknown 2008-05-14	4.3	CVE-2008-2200 BUGTRAQ BID XF
maian_script_world -- maian_recipe	Multiple cross-site scripting (XSS) vulnerabilities in admin/inc/header.php in Maian Recipe 1.2 allow remote attackers to inject arbitrary web script or HTML via the (1) header, (2) header2, (3) header3, (4) header4, (5) header5, (6) header6, (7) header7, (8) header8, and (9) header9 parameters.	unknown 2008-05-14	4.3	CVE-2008-2201 BUGTRAQ BID XF
maian_script_world -- maian_uploader	Multiple cross-site scripting (XSS) vulnerabilities in Maian Uploader 4.0 allow remote attackers to inject arbitrary web script or HTML via the (1) keywords parameter to upload/admin/index.php in a search action, the (2) msg_charset and (3) msg_header9 parameters to admin/inc/header.php, and the (4) keywords parameter to index.php in a search action.	unknown 2008-05-14	4.3	CVE-2008-2202 BUGTRAQ BID XF
maian_script_world -- maian_search	Multiple cross-site scripting (XSS) vulnerabilities in admin/inc/header.php in Maian Search 1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) header, (2) header2, (3) header3, (4) header4, (5) header5, (6) header6, (7) header7, (8) header8, and (9) header9 parameters.	unknown 2008-05-14	4.3	CVE-2008-2204 BUGTRAQ BID
maian_script_world -- maian_music	Multiple cross-site scripting (XSS) vulnerabilities in Maian Music 1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) keywords parameter in a search action to index.php, and the (2) msg_script parameter to admin/inc/footer.php.	unknown 2008-05-14	4.3	CVE-2008-2206 BUGTRAQ BID XF
maian_script_world -- maian_gallery	Cross-site scripting (XSS) vulnerability in admin/index.php in Maian Gallery 2.0 allows remote attackers to inject arbitrary web script or HTML via the keywords parameter in a search action.	unknown 2008-05-14	4.3	CVE-2008-2207 BUGTRAQ BID XF
maianscriptworld -- maian_greeting	Multiple cross-site scripting (XSS) vulnerabilities in admin/inc/header.php in Maian Greeting 2.1 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_script and (2) msg_script2 parameters.	unknown 2008-05-14	4.3	CVE-2008-2209 BUGTRAQ BID XF

maianscriptworld -- maian_support	Multiple cross-site scripting (XSS) vulnerabilities in Maian Support 1.3 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_script, (2) msg_script2, and (3) msg_script3 parameters to admin/inc/footer.php; and the (4) msg_script2 parameter to admin/inc/header.php.	unknown 2008-05-14	4.3	CVE-2008-2210 BUGTRAQ BID XF
maianscriptworld -- maian_guestbook	Multiple cross-site scripting (XSS) vulnerabilities in admin/inc/footer.php in Maian Guestbook 3.2 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_script2 and (2) msg_script3 parameters.	unknown 2008-05-14	4.3	CVE-2008-2211 BUGTRAQ BID XF
maianscriptworld -- maian_cart	Multiple cross-site scripting (XSS) vulnerabilities in Maian Cart 1.1 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_adminheader, (2) msg_adminheader2, (3) msg_adminheader3, (4) msg_adminheader4, and unspecified other parameters to admin/inc/header.php; the (5) msg_script3 and unspecified other parameters to admin/inc/footer.php; and the (6) keywords parameter to index.php in a search action.	unknown 2008-05-14	4.3	CVE-2008-2212 BUGTRAQ BID XF
maianscriptworld -- maian_links	Multiple cross-site scripting (XSS) vulnerabilities in admin/inc/footer.php in Maian Links 3.1 allow remote attackers to inject arbitrary web script or HTML via the (1) msg_script2 and (2) msg_script3 parameters.	unknown 2008-05-14	4.3	CVE-2008-2213 BUGTRAQ BID XF
mario_valdez -- content_management_system	Directory traversal vulnerability in cm/graphie.php in Content Management System 0.6.1 for Phprojekt allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the cm_imgpath parameter.	unknown 2008-05-14	5.0	CVE-2008-2217 MILW0RM BID
mdsjack -- mjguest	Cross-site scripting (XSS) vulnerability in mjguest.php in Mjguest 6.7 GT Rev.01 allows remote attackers to inject arbitrary web script or HTML via the level parameter in a redirect action, possibly involving interface/redirect.htm.php.	unknown 2008-05-13	4.3	CVE-2008-2187 BUGTRAQ BID
mdsjack -- mjguest	Open redirect vulnerability in interface/redirect.htm.php in Mjguest 6.7 GT Rev.01 allows user-assisted remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the goto parameter in a redirect action to mjguest.php. NOTE: this is user-assisted because there is a delay and a notification before redirection occurs.	unknown 2008-05-16	4.3	CVE-2008-2268 BUGTRAQ
Microsoft -- antigen_for_smtp_gateway Microsoft -- Malware Protection Engine Microsoft -- Windows Defender Microsoft -- antigen_for_exchange Microsoft -- diagnostics_and_recovery_toolkit Microsoft -- forefront_client_security Microsoft -- Windows Live OneCare Microsoft -- forefront_security_for_sharepoint Microsoft -- forefront_security_for_exchange_server	Unspecified vulnerability in Microsoft Malware Protection Engine (mpengine.dll) 1.1.3520.0 and 0.1.13.192, as used in multiple Microsoft products, allows context-dependent attackers to cause a denial of service (engine hang and restart) via a crafted file, a different vulnerability than CVE-2008-1438.	unknown 2008-05-13	5.0	CVE-2008-1437 MS BID SECTRACK

Microsoft -- antigen_for_smtp_gateway Microsoft -- Malware Protection Engine Microsoft -- Windows Defender Microsoft -- antigen_for_exchange Microsoft -- diagnostics_and_recovery_toolkit Microsoft -- forefront_client_security Microsoft -- Windows Live OneCare Microsoft -- forefront_security_for_sharepoint Microsoft -- forefront_security_for_exchange_server	Unspecified vulnerability in Microsoft Malware Protection Engine (mpengine.dll) 1.1.3520.0 and 0.1.13.192, as used in multiple Microsoft products, allows context-dependent attackers to cause a denial of service (disk space exhaustion) via a file with "crafted data structures" that trigger the creation of large temporary files, a different vulnerability than CVE-2008-1437.	unknown 2008-05-13	5.0	CVE-2008-1438 MS BID SECTRACK
Nagios -- Nagios	Cross-site scripting (XSS) vulnerability in Nagios allows remote attackers to inject arbitrary web script or HTML via unknown vectors, a different vulnerability than CVE-2007-5624 and CVE-2008-1360.	unknown 2008-05-13	4.3	CVE-2007-5803 SUSE
Nortel -- multimedia_communications_server	Buffer overflow in the Multimedia PC Client in Nortel Multimedia Communication Server (MCS) before Maintenance Release 3.5.8.3 and 4.0.25.3 allows remote attackers to cause a denial of service (crash) via a flood of "extraneous" messages, as demonstrated by the Nessus "Generic flood" denial of service plugin.	unknown 2008-05-14	5.0	CVE-2008-2218 OTHER-REF BID
openkm -- openkm	Unspecified vulnerability in the export feature in OpenKM before 2.0 allows remote attackers to export arbitrary documents via unspecified vectors. NOTE: some of these details are obtained from third party information.	unknown 2008-05-14	5.0	CVE-2008-2226 OTHER-REF
OpenSSL Project -- OpenSSL	OpenSSL 0.9.8c-1 up to 0.9.8g-9 on Debian-based operating systems uses a random number generator that generates predictable numbers, which makes it easier for remote attackers to conduct brute force guessing attacks against cryptographic keys.	unknown 2008-05-13	5.4	CVE-2008-0166 BID
pbcs -- project-based_calendaring_system	Multiple directory traversal vulnerabilities in Project-Based Calendaring System (PBCS) 0.7.1-1 allow remote attackers to read arbitrary files via a .. (dot dot) in the filename parameter to (1) src/yopy_sync.php and (2) system-logger/print_logs.php.	unknown 2008-05-14	5.0	CVE-2008-2215 MILW0RM BID XF
pbcs -- project-based_calendaring_system	Unrestricted file upload vulnerability in src/yopy_upload.php in Project-Based Calendaring System (PBCS) 0.7.1 allows remote authenticated users to upload arbitrary files to tmp/uploads.	unknown 2008-05-14	6.5	CVE-2008-2216 MILW0RM BID XF
php_directory_source -- phpdirectorysource	Multiple SQL injection vulnerabilities in phpDirectorySource 1.1.06, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) lid parameter to show.php and the (2) login parameter to admin.php.	unknown 2008-05-13	6.8	CVE-2008-2177 MILW0RM
PostNuke Software Foundation -- pnEncyclopedia	SQL injection vulnerability in the pnEncyclopedia module 0.2.0 and earlier for PostNuke allows remote attackers to execute arbitrary SQL commands via the id parameter in a display_term action to index.php.	unknown 2008-05-14	6.8	CVE-2008-2191 BUGTRAQ MILW0RM BID XF

QEMU -- QEMU	The drive_init function in QEMU 0.9.1 determines the format of a raw disk image based on the header, which allows local guest users to read arbitrary files on the host by modifying the header to identify a different format, which is used when the guest is restarted.	unknown 2008-05-12	4.9	CVE-2008-2004 MLIST OTHER-REF BID XF
Sazcart -- Sazcart	Multiple PHP remote file inclusion vulnerabilities in SazCart 1.5.1, when register_globals is enabled, allow remote attackers to execute arbitrary PHP code via a URL in the (1) _saz[settings][site_dir] parameter to layouts/default/header.saz.php and the (2) _saz[settings][site_url] parameter to admin/alayouts/default/pages/login.php.	unknown 2008-05-14	6.8	CVE-2008-2224 MILW0RM BID
SCRIPTPHP -- PicEngine	Cross-site scripting (XSS) vulnerability in admin/index.php in Script PHP PicEngine 1.0 allows remote attackers to inject arbitrary web script or HTML via the l parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-16	4.3	CVE-2008-2280 OTHER-REF BID XF
shelter_manager -- animal_shelter_manager	Multiple unspecified vulnerabilities in Robin Rawson-Tetley Animal Shelter Manager (ASM) before 2.2.2 have unknown impact and attack vectors, related to "various areas where security was missing."	unknown 2008-05-13	6.5	CVE-2008-2174 BID XF
SonicWall -- e-mail_security	Cross-site scripting (XSS) vulnerability in SonicWall Email Security 6.1.1 allows remote attackers to inject arbitrary web script or HTML via the Host header in a request to a non-existent web page, which is not properly sanitized in an error page.	unknown 2008-05-12	4.3	CVE-2008-2162 FULLDISC BID SECTRACK XF
Sun -- Java System Web Server	Cross-site scripting (XSS) vulnerability in the search module in Sun Java System Web Server 6.1 before SP9 and 7.0 before Update 2 allows remote attackers to inject arbitrary web script or HTML via unknown parameters in index.jsp.	unknown 2008-05-13	4.3	CVE-2008-2166
toocharger -- smartblog	Directory traversal vulnerability in index.php in SMartBlog (aka SMBlog) 1.3 allows remote attackers to include arbitrary local files via directory traversal sequences in the page parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-13	5.0	CVE-2008-2185
TYPO3 -- TYPO3	Cross-site scripting (XSS) vulnerability in the powermail extension before 1.1.10 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-05-13	4.3	CVE-2008-2182
TYPO3 -- sr_feuser_register Extension	Cross-site scripting (XSS) vulnerability in the sr_feuser_register 1.4.0, 1.6.0, 2.2.1 to 2.2.7, 2.3.0 to 2.3.6, 2.4.0, and 2.5.0 to 2.5.9 extension for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-05-16	6.8	CVE-2008-2274
UUDeview -- UUDeview	uulib/uunconc.c in UUDeview 0.5.20 allows local users to overwrite arbitrary files via a symlink attack on a temporary filename generated by the tempnam function. NOTE: this may be a CVE-2004-2265 regression.	unknown 2008-05-16	4.6	CVE-2008-2266 MLIST OTHER-REF BID

VideoLAN -- VLC	Untrusted search path vulnerability in VideoLAN VLC before 0.9.0 allows local users to execute arbitrary code via a malicious library under the modules/ or plugins/ subdirectories of the current working directory.	unknown 2008-05-12	4.6	CVE-2008-2147 OTHER-REF OTHER-REF
xiph -- libvorbis	Xiph.org libvorbis before 1.0 does not properly check for underpopulated Huffman trees, which allows remote attackers to cause a denial of service (crash) via a crafted OGG file that triggers memory corruption during execution of the _make_decode_tree function.	unknown 2008-05-16	4.3	CVE-2008-2009 OTHER-REF
Xiph.Org -- libvorbis	Integer overflow in residue partition value (aka partvals) evaluation in Xiph.org libvorbis 1.2.0 and earlier allows remote attackers to execute arbitrary code via a crafted OGG file, which triggers a heap overflow.	unknown 2008-05-16	6.8	CVE-2008-1420 OTHER-REF XF
Xiph.Org -- libvorbis	Integer overflow in a certain quantvals and quantlist calculation in Xiph.org libvorbis 1.2.0 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted OGG file with a large virtual space for its codebook, which triggers a heap overflow.	unknown 2008-05-16	6.8	CVE-2008-1423 OTHER-REF XF
zomp -- zomplog	Cross-site scripting (XSS) vulnerability in admin/category.php in Zomplog 3.8.2 allows remote attackers to inject arbitrary web script or HTML via the catname parameter.	unknown 2008-05-13	4.3	CVE-2008-2176 BUGTRAQ BID XF
ZyXEL -- Zywall 100	Cross-site scripting (XSS) vulnerability in ZyXEL ZyWALL 100 allows remote attackers to inject arbitrary web script or HTML via the Referer header, which is not properly handled in a 404 Error page.	unknown 2008-05-13	4.3	CVE-2008-2167 BUGTRAQ FULLDISC BID SECTRACK XF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
freelanceauction.eu -- Freelance Auction Script	Freelance Auction Script 1.0 stores user passwords in plaintext in the tbl_users table, which allows attackers to gain privileges by reading the table.	unknown 2008-05-16	0.0	CVE-2008-2279 MILW0RM XF
Linux -- Kernel	The utimensat system call in Linux kernel 2.6.22 and other versions before 2.6.25.3 does not check file permissions when certain UTIME_NOW and UTIME_OMIT combinations are used, which allows local users to modify file times of arbitrary files, possibly leading to a denial of service.	unknown 2008-05-12	3.6	CVE-2008-2148 OTHER-REF
Microsoft -- Outlook Web Access	Unspecified versions of Microsoft Outlook Web Access (OWA) use the Cache-Control: no-cache HTTP directive instead of no-store, which might cause web browsers that follow RFC-2616 to cache sensitive information.	unknown 2008-05-12	1.9	CVE-2008-2143 CERT-VN BID XF
Microsoft -- ie	Microsoft Internet Explorer 7 can save encrypted pages in the cache even when the DisableCachingOfSSLPages registry setting is enabled, which might allow local users to obtain sensitive information.	unknown 2008-05-12	2.1	CVE-2008-2159 CERT-VN BID

rPath -- appliance_platform_agent	Cross-site request forgery (CSRF) vulnerability in the rootpw plugin in rPath Appliance Platform Agent 2 and 3 allows remote attackers to reset the root password as the administrator via a crafted URL.	unknown 2008-05-12	2.6	CVE-2008-2140 OTHER-REF

Back to top