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
acgv.free -- acgv_news	SQL injection vulnerability in glossaire.php in ACGV News 0.9.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-22	7.5	CVE-2008-2412 OTHER-REF BID XF
alkalinephp -- alkalinephp	AlkalinePHP 0.77.35 and earlier allows remote attackers to bypass authentication and gain administrative access by creating an admin account via a direct request to adduser.php.	unknown 2008-05-20	7.5	CVE-2008-2346 MILW0RM BID
alkalinephp -- alkalinephp	SQL injection vulnerability in thread.php in AlkalinePHP 0.80.00 beta and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-21	7.5	CVE-2008-2395 MILW0RM BID
archangelmgt -- archangel_weblog	SQL injection vulnerability in index.php in Archangel Weblog 0.90.02 and earlier allows remote attackers to execute arbitrary SQL commands via the post_id parameter.	unknown 2008-05-20	7.5	CVE-2008-2356 MILW0RM BID XF

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
CA -- Business Protection Suite CA -- Server Protection Suite CA -- BrightStor ARCserve Backup	Directory traversal vulnerability in caloggerd in CA BrightStor ARCServe Backup 11.0, 11.1, and 11.5 allows remote attackers to append arbitrary data to arbitrary files via directory traversal sequences in unspecified input fields, which are used in log messages. NOTE: this can be leveraged for code execution in many installation environments by writing to a startup file or configuration file.	unknown 2008-05-21	10.0	CVE-2008-2241 OTHER-REF
CA -- BrightStor ARCserve Backup	Multiple buffer overflows in xdr functions in the server in CA BrightStor ARCServe Backup 11.0, 11.1, and 11.5 allow remote attackers to execute arbitrary code, as demonstrated by a stack-based buffer overflow via a long parameter to the xdr_rwsstring function.	unknown 2008-05-21	7.5	CVE-2008-2242 OTHER-REF OTHER-REF
Cisco -- service_control_engine	The SSH server in Cisco Service Control Engine (SCE) before 3.1.6 allows remote attackers to cause a denial of service (device restart or daemon outage) via a high rate of login attempts, aka Bug ID CSCsi68582.	unknown 2008-05-22	7.8	CVE-2008-0534 BID SECTRACK XF
Cisco -- service_control_engine	Unspecified vulnerability in the SSH server in Cisco Service Control Engine (SCE) before 3.1.6 allows remote attackers to cause a denial of service (device instability) via "SSH credentials that attempt to change the authentication method," aka Bug ID CSCsm14239.	unknown 2008-05-22	7.8	CVE-2008-0535 BID SECTRACK XF
Cisco -- service_control_engine	Unspecified vulnerability in the SSH server in Cisco Service Control Engine (SCE) before 3.0.7, and 3.1.x before 3.1.0,	unknown 2008-05-22	7.8	CVE-2008-0536 BID SECTRACK XF

	allows remote attackers to cause a denial of service (management interface outage) via SSH traffic that occurs during management operations and triggers "illegal I/O operations," aka Bug ID CSCsh49563.			
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 -- IOS T Cisco -- IOS S Cisco -- IOS XR	Multiple unspecified vulnerabilities in the SSH server in Cisco IOS 12.4 allow remote attackers to cause a denial of service (device restart) via unknown vectors, aka Bug ID (1) CSCsk42419, (2) CSCsk60020, and (3) CSCsh51293.	unknown 2008-05-22	7.1	CVE-2008-1159 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) 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	7.8	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	7.8	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	unknown 2008-05-16	7.8	CVE-2008-1745 CISCO BID SECTRACK XF

	malformed header, aka Bug ID CSCsi48115.			
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	7.8	CVE-2008-1746 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 -- Unified Communications Manager Cisco -- Unified CallManager	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 SECTRACK XF
Cisco -- unified_customer_voice_portal	Unspecified vulnerability in Cisco Unified Customer Voice Portal (CVP) 4.0.x before 4.0(2)_ES14, 4.1.x before 4.1(1)_ES11, and 7.x before 7.0(1) allows remote authenticated users with administrator role privileges to create, modify, or delete a superuser account.	unknown 2008-05-22	9.0	CVE-2008-2053 BID 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	unknown 2008-05-16	7.5	CVE-2008-2267 MILW0RM OTHER-REF VIM BID

	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/.			XF
cmsnx -- 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
cmsnx -- 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
codeplex -- subsonic	SubSonic allows remote attackers to bypass pagesize limits and cause a denial of service (CPU consumption) via a pageindex (aka data page number) of -1.	unknown 2008-05-21	7.8	CVE-2008-2391 BUGTRAQ OTHER-REF OTHER-REF
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	7.5	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
entertainmentscript -- entertainmentscript	SQL injection vulnerability in play.php in EntertainmentScript 1.4.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-05-21	7.5	CVE-2008-2393 MILW0RM BID
fichive -- fichive	SQL injection vulnerability in index.php in FicHive 1.0 allows remote attackers to execute arbitrary SQL commands via the	unknown 2008-05-22	7.5	CVE-2008-2416 MILW0RM BID

	category parameter in a Fiction action.			
fireftp -- fireftp	Directory traversal vulnerability in the FireFTP add-on before 0.98.20080518 for Firefox allows remote FTP servers to create or overwrite arbitrary files via ..\ (dot dot backslash) sequences in responses to (1) MLSD and (2) LIST commands, a related issue to CVE-2002-1345. NOTE: this can be leveraged for code execution by writing to a Startup folder.	unknown 2008-05-22	9.3	CVE-2008-2399 OTHER-REF OTHER-REF XF
Foxit -- reader	Stack-based buffer overflow in Foxit Reader before 2.3 build 2912 allows user-assisted remote attackers to execute arbitrary code via a crafted PDF file, related to the util.printf JavaScript function and floating point specifiers in format strings.	unknown 2008-05-21	9.3	CVE-2008-1104 BUGTRAQ BID XF
freelanceauction -- 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
GNU -- GnuTLS	The _gnutls_server_name_recv_params function in lib/ext_server_name.c in libgnutls in gnutls-serv in GnuTLS before 2.2.4 does not properly calculate the number of Server Names in a TLS 1.0 Client Hello message during extension handling, which allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a zero value for the length of Server Names, which leads to a buffer overflow in session resumption data in the pack_security_parameters function, aka GNUTLS-SA-2008-1-1.	unknown 2008-05-21	10.0	CVE-2008-1948 BUGTRAQ MLIST MLIST MLIST MLIST MLIST OTHER-REF OTHER-REF REDHAT REDHAT XF
gnugallery -- gnugallery	Directory traversal vulnerability in admin.php in GNU/Gallery 1.1.1.0 and earlier allows remote attackers to include and execute arbitrary	unknown 2008-05-20	7.5	CVE-2008-2353 MILW0RM BID

	local files via a .. (dot dot) in the show parameter.			
how2asp -- webboard	SQL injection vulnerability in showQAnswer.asp in How2ASP.net Webboard 4.1 allows remote attackers to execute arbitrary SQL commands via the qNo parameter.	unknown 2008-05-22	7.5	CVE-2008-2417 MILW0RM BID
HP -- Software Update	Hpufunction.dll 4.0.0.1 in HP Software Update exposes the unsafe (1) ExecuteAsync and (2) Execute methods, which allows remote attackers to execute arbitrary code via an absolute pathname in the first argument.	unknown 2008-05-21	7.5	CVE-2008-2390 MILW0RM
IBM -- Lotus Domino	Stack-based buffer overflow in the Web Server service in IBM Lotus Domino before 7.0.3 FP1, and 8.x before 8.0.1, allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a long Accept-Language HTTP header.	unknown 2008-05-22	10.0	CVE-2008-2240 VIM VIM BID XF
meltingicefs -- melting_ice_file_system	MeltingIce File System 1.0 allows remote attackers to bypass application authentication, create new user accounts, and exceed application quotas via a direct request to admin/adduser.php.	unknown 2008-05-20	7.5	CVE-2008-2348 MILW0RM BID
mypicgallery -- mypicgallery	MyPicGallery 1.0 allows remote attackers to bypass application authentication and gain administrative access by setting the userID parameter to "admin" in a direct request to admin/addUser.php.	unknown 2008-05-20	7.5	CVE-2008-2347 MILW0RM BID
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
redhat -- enterprise_linux redhat -- fedora	Memory leak in a certain Red Hat patch, applied to vsftpd 2.0.5 on Red Hat Enterprise Linux (RHEL)	unknown 2008-05-22	7.1	CVE-2007-5962 MLIST MLIST

	5 and Fedora 6 through 8, and on Foresight Linux and rPath appliances, allows remote attackers to cause a denial of service (memory consumption) via a large number of CWD commands, as demonstrated by an attack on a daemon with the deny_file configuration option.			MLIST OTHER-REF BID SECTRACK
Stunnel -- Stunnel	Unspecified vulnerability in stunnel before 4.23, when running as a service on Windows, allows local users to gain privileges via unknown attack vectors.	unknown 2008-05-22	7.2	CVE-2008-2400 MLIST
tagworx -- tagworx_cms	Multiple SQL injection vulnerabilities in TAGWORX.CMS 3.00.02 allow remote attackers to execute arbitrary SQL commands via the (1) cid parameter to contact.php and the (2) nid parameter to news.php.	unknown 2008-05-21	7.5	CVE-2008-2394 MILW0RM OTHER-REF
thomas_voecking -- internet_photoshow	admin.php in Internet Photoshow and Internet Photoshow Special Edition (SE) allows remote attackers to bypass authentication by setting the login_admin cookie to true.	unknown 2008-05-18	7.5	CVE-2008-2282 MILW0RM BID XF
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
wajox_software -- mircrossys_cms	PHP remote file inclusion vulnerability in index.php in Wajox Software microSSys CMS 1.5 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in an arbitrary element of the PAGES array parameter.	unknown 2008-05-21	7.5	CVE-2008-2396 MILW0RM
webmanager-pro -- cms_webmanager-pro	Multiple SQL injection vulnerabilities in index.php in CMS WebManager-Pro allow remote attackers to execute	unknown 2008-05-20	7.5	CVE-2008-2351 MILW0RM BID

	arbitrary SQL commands via the (1) lang_id and (2) menu_id parameters.			
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	9.3	CVE-2008-1423 OTHER-REF XF
zomp -- zomplog	Zomplog 3.8.2 and earlier allows remote attackers to gain administrative access by creating an admin account via a direct request to install/newuser.php with the admin parameter set to 1.	unknown 2008-05-20	7.5	CVE-2008-2349 MILW0RM BID XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
acgv.free -- acgv_news	Cross-site scripting (XSS) vulnerability in glossaire.php in ACGV News 0.9.1 allows remote attackers to inject arbitrary web script or HTML via the id parameter.	unknown 2008-05-22	4.3	CVE-2008-2413 OTHER-REF BID XF
aguestbook -- an_guestbook	Cross-site scripting (XSS) vulnerability in send_email.php in AN Guestbook (ANG) 0.4 allows remote attackers to inject arbitrary web script or HTML via the postid parameter.	unknown 2008-05-22	4.3	CVE-2008-2414 OTHER-REF BID XF
Apple -- iCal	Apple iCal 3.0.1 on Mac OS X allows remote CalDAV servers, and user-assisted remote attackers, to cause a denial of service (NULL pointer dereference and application crash) or possibly execute arbitrary code via a .ics file containing (1) a large 16-bit integer on a TRIGGER line, or (2) a large integer in a COUNT field on an RRULE line. NOTE: this might be a duplicate of CVE-2008-1035.	unknown 2008-05-22	4.3	CVE-2008-2006 BUGTRAQ OTHER-REF BID
Apple -- iCal	Apple iCal 3.0.1 on Mac OS X allows remote CalDAV servers, and user-assisted remote attackers, to trigger	unknown 2008-05-22	4.3	CVE-2008-2007 BUGTRAQ OTHER-REF

	memory corruption or possibly execute arbitrary code via an "ATTACH;VALUE=URI:S=osumi" line in a .ics file, which triggers a "resource liberation" bug.			BID
AppServ Open Project -- AppServ	Cross-site scripting (XSS) vulnerability in index.php in AppServ Open Project 2.5.10 and earlier allows remote attackers to inject arbitrary web script or HTML via the appservlang parameter.	unknown 2008-05-21	4.3	CVE-2008-2398 BUGTRAQ BID
bcoos -- bcoos	Directory traversal vulnerability in highlight.php in bcoos 1.0.9 through 1.0.13 allows remote attackers to read arbitrary files via (1) .. (dot dot) or (2) C: folder sequences in the file parameter.	unknown 2008-05-20	5.0	CVE-2008-2350 OTHER-REF BID 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
DigitalHive -- DigitalHive	Directory traversal vulnerability in template/purpletech/base_include.php in DigitalHive (aka hive) 2.0 RC2 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the page parameter.	unknown 2008-05-22	6.8	CVE-2008-2415 OTHER-REF BID XF
dotcms -- dotcms	Cross-site scripting (XSS) vulnerability in search-results.dot in dotCMS 1.x allows remote attackers to inject arbitrary web script or HTML via the search_query parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-05-21	4.3	CVE-2008-2397
GForge -- GForge	The write_array_file function in utils/include.pl in GForge 4.5.14 updates configuration files by truncating them to zero length and then writing new data, which might allow attackers to bypass intended access restrictions or have unspecified other impact in opportunistic circumstances.	unknown 2008-05-18	4.6	CVE-2008-0167 OTHER-REF BID XF
GNU -- GnuTLS	The _gnutls_recv_client_kx_message function in lib/gnutls_kx.c in libgnutls in gnutls-serv in GnuTLS before 2.2.4	unknown 2008-05-21	6.8	CVE-2008-1949 BUGTRAQ MLIST

	continues to process Client Hello messages within a TLS message after one has already been processed, which allows remote attackers to cause a denial of service (NULL dereference and crash) via a TLS message containing multiple Client Hello messages, aka GNUTLS-SA-2008-1-2.			MLIST MLIST MLIST MLIST MLIST OTHER-REF OTHER-REF REDHAT REDHAT XF
GNU -- GnuTLS	Integer signedness error in the _gnutls_ciphertext2compressed function in lib/gnutls_cipher.c in libgnutls in GnuTLS before 2.2.4 allows remote attackers to cause a denial of service (buffer over-read and crash) via a certain integer value in the Random field in an encrypted Client Hello message within a TLS record with an invalid Record Length, which leads to an invalid cipher padding length, aka GNUTLS-SA-2008-1-3.	unknown 2008-05-21	5.0	CVE-2008-1950 BUGTRAQ MLIST MLIST MLIST MLIST OTHER-REF OTHER-REF REDHAT REDHAT BID XF
HP -- HP-UX	Unspecified vulnerability in useradd on HP-UX B.11.11, B.11.23, and B.11.31 allows local users to access arbitrary files and directories via unspecified vectors.	unknown 2008-05-21	6.3	CVE-2008-1660 HP BID XF
IBM -- Lotus Domino Web Server	Cross-site scripting (XSS) vulnerability in the servlet engine and Web container in the Web Server service in IBM Lotus Domino before 7.0.3 FP1, and 8.x before 8.0.1, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-05-22	4.3	CVE-2008-2410 OTHER-REF XF
matisbt -- 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	6.8	CVE-2008-2276 OTHER-REF
Matt Kimball and Roger Wolff -- mtr	Stack-based buffer overflow in the split_redraw function in split.c in mtr before 0.73, when invoked with the -p (aka --split) option, allows remote attackers to execute arbitrary code via a crafted DNS PTR record. NOTE: it could be argued that this is a vulnerability in the ns_name_ntop function in resolv/ns_name.c in glibc and the proper fix should be in glibc; if	unknown 2008-05-21	6.8	CVE-2008-2357 BUGTRAQ FULLDISC MLIST MLIST MLIST OTHER-REF OTHER-REF

	so, then this should not be treated as a vulnerability in mtr.			
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
oued -- 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
photostockplus -- photostockplus_uploader_tool	Multiple stack-based buffer overflows in the PhotoStockPlus Uploader Tool ActiveX control (PSPUploader.ocx) allow remote attackers to execute arbitrary code via unspecified initialization parameters.	unknown 2008-05-20	6.8	CVE-2008-0957 CERT-VN BID
Sazcart -- Sazcart	SQL injection vulnerability in index.php in SazCart 1.5.1 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the prodid parameter in a details action.	unknown 2008-05-22	6.8	CVE-2008-2411 BUGTRAQ MILW0RM BID
smeego -- smeego	Directory traversal vulnerability in index.php in Smeego 1.0, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang cookie.	unknown 2008-05-20	6.8	CVE-2008-2352 MILW0RM BID
Snort -- Snort	preprocessors/spp_frag3.c in Sourcefire Snort before 2.8.1 does not properly identify packet fragments that have dissimilar TTL values, which allows remote attackers to bypass detection rules by using a different TTL for each fragment.	unknown 2008-05-22	6.8	CVE-2008-1804 IDEFENSE OTHER-REF OTHER-REF BID SECTRACK
testmaker -- testmaker	Unspecified vulnerability in the data export function in testMaker before	unknown 2008-05-20	5.0	CVE-2008-2354

	3.0p10 allows test authors to obtain access to export data via unknown vectors.			
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
WordPress -- WordPress	Unrestricted file upload vulnerability in WordPress 2.5.1 and earlier might allow remote authenticated administrators to upload and execute arbitrary PHP files via the Upload section in the Write Tabs area of the dashboard.	unknown 2008-05-21	6.5	CVE-2008-2392 BUGTRAQ BID
wr-script -- wr-meeting	Directory traversal vulnerability in index.php in WR-Meeting 1.0, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the msnum parameter in a coment event.	unknown 2008-05-20	6.8	CVE-2008-2355 MILW0RM BID
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	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	4.3	CVE-2008-1419 OTHER-REF XF XF
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

Back to top

There were no low vulnerabilities recorded this week.