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
Adam Scheinberg -- Flip	PHP remote file inclusion vulnerability in config.php in Adam Scheinberg Flip 3.0 allows remote attackers to execute arbitrary PHP code via a URL in the incpath parameter.	unknown 2008-07-25	7.5	CVE-2008-3311 BUGTRAQ BID XF
alphadmin -- alphadmin_cms	AlphAdmin CMS 1.0.5/03 allows remote attackers to bypass authentication and gain administrative access by setting the aa_login cookie value to 1. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	7.5	CVE-2008-3300 BID
AlstraSoft -- video_share_enterprise	SQL injection vulnerability in album.php in AlstraSoft Video Share Enterprise 4.51 allows remote attackers to execute arbitrary SQL commands via the UID parameter, a different vector than CVE-2007-4086.	unknown 2008-07-30	7.5	CVE-2008-3386 MILW0RM BID
atomphotoblog -- atomphotoblog	SQL injection vulnerability in atomPhotoBlog.php in Atom PhotoBlog 1.0.9.1 and 1.1.5b1 allows remote attackers to execute arbitrary SQL commands via the photoId parameter in a show action.	unknown 2008-07-28	7.5	CVE-2008-3351 MILW0RM XF
axesstel -- akw-d800	The Axesstel AXW-D800 modem with D2_ETH_109_01_VEBR Jun-14-2006 software does not require authentication for (1) etc/config/System.html, (2) etc/config/Network.html, (3) etc/config/Security.html, (4) cgi-bin/sysconf.cgi, and (5) cgi-bin/route.cgi, which allows remote attackers to change the modem's configuration via direct requests.	unknown 2008-07-31	10.0	CVE-2008-3411 BUGTRAQ BID XF
Blue Coat Systems -- K9 Web Protection Blue Coat Systems -- filter	Multiple stack-based buffer overflows in the filter service (aka k9filter.exe) in Blue Coat K9 Web Protection 3.2.44 with Filter 3.2.32 allow (1) remote attackers to execute arbitrary code via a long HTTP Referer header to the K9 Web Protection Administration interface and (2) man-in-the-middle attackers to execute arbitrary code via an HTTP response with a long HTTP version field.	unknown 2008-08-01	9.3	CVE-2007-2952
Brandon Tallent -- phptest	SQL injection vulnerability in picture.php in phpTest 0.6.3 allows remote attackers to execute arbitrary SQL commands via the image_id parameter.	unknown 2008-07-30	7.5	CVE-2008-3377 MILW0RM BID

Camera Life -- Camera Life	SQL injection vulnerability in sitemap.xml.php in Camera Life 2.6.2 allows remote attackers to execute arbitrary SQL commands via the id parameter in a photos action.	unknown 2008-07-28	7.5	CVE-2008-3355 MILW0RM
cce-interact -- interact	Multiple directory traversal vulnerabilities in help/help.php in Interact Learning Community Environment Interact 2.4.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) module and (2) file parameters.	unknown 2008-07-30	7.5	CVE-2008-3384 BUGTRAQ MILW0RM OTHER-REF BID XF
condor_project -- condor	Condor before 7.0.4 does not properly handle wildcards in the ALLOW_WRITE, DENY_WRITE, HOSTALLOW_WRITE, or HOSTDENY_WRITE configuration variables in authorization policy lists, which might allow remote attackers to bypass intended access restrictions.	unknown 2008-07-31	7.5	CVE-2008-3424 OTHER-REF BID XF
Dokeos -- E-Learning System	Directory traversal vulnerability in user_portal.php in the Dokeos E-Learning System 1.8.5 on Windows allows remote attackers to include and execute arbitrary local files via a ..\ (dot dot backslash) in the include parameter.	unknown 2008-07-30	7.5	CVE-2008-3363 BUGTRAQ MILW0RM OTHER-REF
e-topbiz -- shopcart_dx	SQL injection vulnerability in product_detail.php in ShopCart DX allows remote attackers to execute arbitrary SQL commands via the pid parameter.	unknown 2008-07-28	7.5	CVE-2008-3346 MILW0RM
easy-script -- def_blog	Multiple SQL injection vulnerabilities in Def-Blog 1.0.3 allow remote attackers to execute arbitrary SQL commands via the article parameter to (1) comaddok.php and (2) comlook.php.	unknown 2008-07-30	7.5	CVE-2008-3388 BUGTRAQ BID XF
ecshop -- epshop	SQL injection vulnerability in Comsenz EPShop (aka ECShop) before 3.0 allows remote attackers to execute arbitrary SQL commands via the pid parameter in a (1) pro_show or (2) disppro action to the default URI.	unknown 2008-07-31	7.5	CVE-2008-3412 MILW0RM BID XF
EMC -- centera_universal_access	SQL injection vulnerability in the CUA Login Module in EMC Centera Universal Access (CUA) 4.0_4735.p4 allows remote attackers to execute arbitrary SQL commands via the user (user name) field.	unknown 2008-07-30	7.5	CVE-2008-3370 FULLDISC BID SECTRACK XF
Epic Games -- unreal_tournament_3	Buffer overflow in Unreal Tournament 3 1.3beta4 and earlier allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a UDP packet containing a large value in a certain size field, followed by a data string of that size, aka attack 1 in ut3mendo.c.	unknown 2008-07-31	7.5	CVE-2008-3409 OTHER-REF OTHER-REF BID
eps -- probe_builder HP -- openview_internet_services	The Probe Builder Service (aka PBOVISServer.exe) in European Performance Systems (EPS) Probe Builder 2.2 before A.02.20.901, as used in HP OpenView Internet Services (OVIS) on Windows, allows remote attackers to kill arbitrary processes via a process ID number in an unspecified opcode.	unknown 2008-07-29	7.8	CVE-2008-1667 IDEFENSE HP
eSyndicat -- esyndicat	eSyndiCat 1.6 allows remote attackers to bypass authentication and gain administrative access by setting the admin_lng cookie value to 1. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	7.5	CVE-2008-3299 BID
Eyeball Networks -- Eyeball Messenger SDK	Buffer overflow in the CoVideoWindow.ocx ActiveX control 5.0.907.1 in Eyeball MessengerSDK, as used in products such as SiOL Komunikator 1.3, allows remote attackers to execute arbitrary code via a large argument supplied to the BGColor method. NOTE: this might only be a vulnerability in certain insecure configurations of Internet	unknown 2008-07-31	9.0	CVE-2008-3430 OTHER-REF BID XF

	Explorer.			
fizzmedia_negativekarma -- fizzmedia	SQL injection vulnerability in comment.php in Fizzmedia 1.51.2 allows remote attackers to execute arbitrary SQL commands via the mid parameter.	unknown 2008-07-30	7.5	CVE-2008-3378 MILW0RM BID
giulio_ganci -- wp_downloads_manager WordPress -- wp_downloads_manager	Unrestricted file upload vulnerability in upload.php in the Giulio Ganci Wp Downloads Manager module 0.2 for WordPress allows remote attackers to execute arbitrary code by uploading a file with an executable extension via the upfile parameter, then accessing it via a direct request to the file in wp-content/plugins/downloads-manager/upload/.	unknown 2008-07-30	10.0	CVE-2008-3362 MILW0RM BID XF
greatclone -- getacoder_clone	SQL injection vulnerability in search_form.php in Getacoder Clone allows remote attackers to execute arbitrary SQL commands via the sb_protype parameter.	unknown 2008-07-30	7.5	CVE-2008-3372 MILW0RM BID
Gregarius -- Gregarius	SQL injection vulnerability in ajax.php in Gregarius 0.5.4 and earlier allows remote attackers to execute arbitrary SQL commands via the rsargs array parameter in an __exp__getFeedContent action.	unknown 2008-07-30	7.5	CVE-2008-3374 OTHER-REF OTHER-REF
HP -- system_administration_manager	Unspecified vulnerability in the HP System Administration Manager (SAM) on HP-UX B.11.11 and B.11.23, when used to configure NFS, might allow remote attackers to read or modify arbitrary files, related to an "empty systems list."	unknown 2008-08-01	10.0	CVE-2008-1662 HP BID SECTRACK
hscripts -- hiox_random_ad	PHP remote file inclusion vulnerability in hioxRandomAd.php in HIOX Random Ad (HRA) 1.3 allows remote attackers to execute arbitrary PHP code via a URL in the hm parameter.	unknown 2008-07-31	7.5	CVE-2008-3401 BUGTRAQ MILW0RM
hscripts -- hiox_random_ad	Multiple PHP remote file inclusion vulnerabilities in HIOX Browser Statistics (HBS) 2.0 allow remote attackers to execute arbitrary PHP code via a URL in the hm parameter to (1) hioxupdate.php and (2) hioxstats.php.	unknown 2008-07-31	7.5	CVE-2008-3402 BUGTRAQ MILW0RM
IceBB -- IceBB	SQL injection vulnerability in modules/members.php in IceBB before 1.0-rc9.3 allows remote attackers to execute arbitrary SQL commands via the username parameter in a members action to index.php, related to an incorrect protection mechanism in the clean_string function in includes/functions.php.	unknown 2008-07-31	7.5	CVE-2008-3416 MILW0RM OTHER-REF BID
infomining -- bookmine	SQL injection vulnerability in events.cfm in BookMine allows remote attackers to execute arbitrary SQL commands via the events_id parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-31	7.5	CVE-2008-3393
intellitamper -- intellitamper	Stack-based buffer overflow in the HTML parser in IntelliTamper 2.0.7 allows remote attackers to execute arbitrary code via a long URL in the HREF attribute of an A element, a different vulnerability than CVE-2006-2494.	unknown 2008-07-29	9.3	CVE-2008-3360 MILW0RM MILW0RM MILW0RM BID SECTRACK
intellitamper -- intellitamper	Stack-based buffer overflow in IntelliTamper 2.07 allows remote web sites to execute arbitrary code via a long HTTP Server header.	unknown 2008-07-29	7.5	CVE-2008-3361 MILW0RM BID
Jamroom -- Jamroom	The jrCookie function in includes/jamroom-misc.inc.php in JamRoom before 3.4.0 allows remote attackers to bypass authentication and gain administrative access via a boolean value within serialized data in a JMU_Cookie cookie.	unknown 2008-07-30	7.5	CVE-2008-3375 BUGTRAQ OTHER-REF OTHER-REF BID
Jamroom -- Jamroom	Multiple unspecified vulnerabilities in JamRoom before 3.4.0 have unknown impact and attack vectors.	unknown 2008-07-30	10.0	CVE-2008-3376 OTHER-REF OTHER-REF BID

jobbex -- jobsite	Multiple SQL injection vulnerabilities in search_result.cfm in Jobbex JobSite allow remote attackers to execute arbitrary SQL commands via the (1) jobcountryid and (2) jobstateid parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-28	7.5	CVE-2008-3341 BID XF
maian_script_world -- maian_search	admin/index.php in Maian Search 1.1 and earlier allows remote attackers to bypass authentication and gain administrative access by sending an arbitrary search_cookie cookie.	unknown 2008-07-25	7.5	CVE-2008-3317 MILW0RM OTHER-REF BID
maian_script_world -- maian_uploader	admin/index.php in Maian Uploader 4.0 and earlier allows remote attackers to bypass authentication and gain administrative access by sending an arbitrary uploader_cookie cookie.	unknown 2008-07-25	7.5	CVE-2008-3321 MILW0RM OTHER-REF BID
Mobius -- mimsy_xg	Multiple SQL injection vulnerabilities in Möbius for Mimsy XG 1.4.4.1 and earlier allow remote attackers to execute arbitrary SQL commands via (1) the id parameter in browse.php and (2) the s parameter in detail.php.	unknown 2008-07-31	7.5	CVE-2008-3427 MILW0RM
MojoScripts -- mojoclassifieds	SQL injection vulnerability in mojoClassified.cgi in MojoClassifieds 2.0 allows remote attackers to execute arbitrary SQL commands via the cat_a parameter.	unknown 2008-07-30	7.5	CVE-2008-3382 MILW0RM SECUNIA XF
MojoScripts -- mojoauto	SQL injection vulnerability in mojoAuto.cgi in MojoAuto allows remote attackers to execute arbitrary SQL commands via the cat_a parameter in a browse action.	unknown 2008-07-30	7.5	CVE-2008-3383 MILW0RM XF
MojoScripts -- mojopersonals	SQL injection vulnerability in mojoClassified.cgi in MojoPersonals allows remote attackers to execute arbitrary SQL commands via the cat parameter.	unknown 2008-07-31	7.5	CVE-2008-3403 MILW0RM BID XF
MyioSoft -- easypublish	SQL injection vulnerability in staticpages/easypublish/index.php in MyioSoft EasyPublish 3.0tr (trial edition) allows remote attackers to execute arbitrary SQL commands via the read parameter in a search action.	unknown 2008-07-28	7.5	CVE-2008-3343 BUGTRAQ BID XF
MyioSoft -- easydynamicpages	SQL injection vulnerability in staticpages/easycalendar/index.php in MyioSoft EasyDynamicPages 3.0 trial edition (tr) allows remote attackers to execute arbitrary SQL commands via the year parameter.	unknown 2008-07-28	7.5	CVE-2008-3347 BUGTRAQ BID XF
nersoft -- live_music_plus	SQL injection vulnerability in index.php in Live Music Plus 1.1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter in a Singer action.	unknown 2008-07-28	7.5	CVE-2008-3352 MILW0RM
Netapp -- data_ontap	Multiple unspecified vulnerabilities in NetApp Data ONTAP, as used on NetApp and IBM eServer platforms, allow remote attackers to execute arbitrary commands, cause a denial of service (system crash), or obtain sensitive information, probably related to insufficient access control for HTTP requests. NOTE: this may overlap CVE-2008-3160.	unknown 2008-07-28	10.0	CVE-2008-3349 OTHER-REF OTHER-REF OTHER-REF CERT-VN
Owl -- intranet_knowledgebase	SQL injection vulnerability in register.php in Steve Bourgeois and Chris Vincent Owl Intranet Knowledgebase 0.95 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-29	7.5	CVE-2008-3359
phpfootball -- phpfootball	SQL injection vulnerability in show.php in PHPFootball 1.6 allows remote attackers to execute arbitrary SQL commands via the dbtable parameter.	unknown 2008-07-30	7.5	CVE-2008-3387 MILW0RM BID

				XF
phpLinkat -- phpLinkat	SQL injection vulnerability in showcat.php in phpLinkat 0.1 allows remote attackers to execute arbitrary SQL commands via the catid parameter.	unknown 2008-07-31	7.5	CVE-2008-3406 MILW0RM BID XF
Pixelpost -- Pixelpost	Directory traversal vulnerability in index.php in Pixelpost 1.7.1 on Windows, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the language_full parameter.	unknown 2008-07-30	7.5	CVE-2008-3365 BUGTRAQ MILW0RM
Pligg -- Pligg CMS	SQL injection vulnerability in story.php in Pligg CMS Beta 9.9.0 allows remote attackers to execute arbitrary SQL commands via the id parameter. NOTE: this might overlap CVE-2008-1774.	unknown 2008-07-30	7.5	CVE-2008-3366 MILW0RM XF
preproject -- pre_survey_poll	SQL injection vulnerability in default.asp in Pre Survey Poll allows remote attackers to execute arbitrary SQL commands via the catid parameter.	unknown 2008-07-25	7.5	CVE-2008-3310 MILW0RM
PunBB -- PunBB	Unspecified vulnerability in PunBB before 1.2.19 allows remote attackers to inject arbitrary SMTP commands via unknown vectors.	unknown 2008-07-27	10.0	CVE-2008-3335 OTHER-REF
Python Software Foundation -- Python	Multiple integer overflows in Python 2.5.2 and earlier allow context-dependent attackers to have an unknown impact via vectors related to the (1) stringobject, (2) unicodeobject, (3) bufferobject, (4) longobject, (5) tupleobject, (6) stropmodule, (7) gcmodule, and (8) mmapmodule modules.	unknown 2008-08-01	7.5	CVE-2008-2315 OTHER-REF OTHER-REF GENTOO
Python Software Foundation -- Python	Integer overflow in _hashopenssl.c in the hashlib module in Python 2.5.2 and earlier might allow context-dependent attackers to defeat cryptographic digests, related to "partial hashlib hashing of data exceeding 4GB."	unknown 2008-08-01	7.5	CVE-2008-2316 OTHER-REF OTHER-REF GENTOO
Python Software Foundation -- Python	Multiple buffer overflows in Python 2.5.2 and earlier on 32bit platforms allow context-dependent attackers to cause a denial of service (crash) or have unspecified other impact via a long string that leads to incorrect memory allocation during Unicode string processing, related to the unicode_resize function and the PyMem_RESIZE macro.	unknown 2008-08-01	7.5	CVE-2008-3142 OTHER-REF OTHER-REF OTHER-REF GENTOO
Python Software Foundation -- Python	Multiple integer overflows in Python before 2.5.2 might allow context-dependent attackers to have an unknown impact via vectors related to (1) Include/pymem.h; (2) _csv.c, (3) _struct.c, (4) arraymodule.c, (5) audioop.c, (6) binascii.c, (7) cPickle.c, (8) cStringIO.c, (9) cjkcodecs/multibytecodec.c, (10) datetimemodule.c, (11) md5.c, (12) rgbimgmodule.c, and (13) stropmodule.c in Modules/; (14) bufferobject.c, (15) listobject.c, and (16) obmalloc.c in Objects/; (17) Parser/node.c; and (18) asdl.c, (19) ast.c, (20) bltinmodule.c, and (21) compile.c in Python/, as addressed by "checks for integer overflows, contributed by Google."	unknown 2008-08-01	7.5	CVE-2008-3143 OTHER-REF OTHER-REF OTHER-REF OTHER-REF GENTOO
Real -- RealPlayer	Heap-based buffer overflow in the Shockwave Flash (SWF) frame handling in RealNetworks RealPlayer 10.5 Build 6.0.12.1483 might allow remote attackers to execute arbitrary code via a crafted SWF file.	unknown 2008-07-28	9.3	CVE-2007-5400 BUGTRAQ OTHER-REF
Real -- RealPlayer	Unspecified vulnerability in RealNetworks RealPlayer Enterprise, RealPlayer 10, and RealPlayer 10.5 before build 6.0.12.1675 has unknown impact and attack vectors, probably related to accessing local files, aka a "Local resource reference vulnerability."	unknown 2008-07-28	10.0	CVE-2008-3064 OTHER-REF
Real -- RealPlayer	Stack-based buffer overflow in a certain ActiveX control in rjbdll.dll in RealNetworks RealPlayer Enterprise, RealPlayer 10, and RealPlayer 10.5 before build 6.0.12.1675 allows	unknown 2008-07-28	9.3	CVE-2008-3066 OTHER-REF OTHER-REF

	remote attackers to execute arbitrary code by importing a file into a media library and then deleting this file.			
redhat -- nfs_utils	A certain Red Hat build script for nfs-utils before 1.0.9-35z.el5_2 on Red Hat Enterprise Linux (RHEL) 5 omits TCP wrappers support, which might allow remote attackers to bypass intended access restrictions.	unknown 2008-08-01	7.5	CVE-2008-1376 REDHAT BID
redhat -- cygwin	setup.exe before 2.573.2.3 in Cygwin does not properly verify the authenticity of packages, which allows remote Cygwin mirror servers or man-in-the-middle attackers to execute arbitrary code via a package list containing the MD5 checksum of a Trojan horse package.	unknown 2008-07-28	10.0	CVE-2008-3323 BUGTRAQ OTHER-REF OTHER-REF
RunCMS -- newbb_plus_module RunCMS -- RunCMS	Multiple PHP remote file inclusion vulnerabilities in the Newbb Plus (newbb_plus) module 0.93 in RunCMS 1.6.1 allow remote attackers to execute arbitrary PHP code via a URL in the (1) bbPath[path] parameter to votepolls.php and the (2) bbPath[root_theme] parameter to config.php, different vectors than CVE-2006-0659. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-28	7.5	CVE-2008-3354 OTHER-REF BID XF
Social Engine -- Social Engine	Multiple SQL injection vulnerabilities in SocialEngine (SE) before 2.83 allow remote attackers to execute arbitrary SQL commands via (1) an se_user cookie to include/class_user.php or (2) an se_admin cookie to include/class_admin.php.	unknown 2008-07-25	7.5	CVE-2008-3297 BUGTRAQ BID XF
talkback -- TalkBack	Directory traversal vulnerability in install/help.php in TalkBack 2.3.5 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the language parameter.	unknown 2008-07-30	7.5	CVE-2008-3371 MILW0RM BID XF
Trend Micro -- OfficeScan	Buffer overflow in the ObjRemoveCtrl Class ActiveX control in OfficeScanRemoveCtrl.dll 7.3.0.1020 in Trend Micro OfficeScan Corp Edition Web-Deployment 7.3 build 1343 Patch 4 allows remote attackers to execute arbitrary code via a long string in the Server property, and possibly other properties. NOTE: some of these details are obtained from third party information.	unknown 2008-07-30	9.3	CVE-2008-3364 MILW0RM BID XF
twibright -- links	Unspecified vulnerability in Links before 2.1, when "only proxies" is enabled, has unknown impact and attack vectors related to providing "URLs to external programs."	unknown 2008-07-27	9.3	CVE-2008-3329 OTHER-REF
ViArt -- viart_shop	SQL injection vulnerability in products_rss.php in ViArt Shop 3.5 and earlier allows remote attackers to execute arbitrary SQL commands via the category_id parameter.	unknown 2008-07-30	7.5	CVE-2008-3369 BUGTRAQ MILW0RM OTHER-REF BID
willo -- trio	SQL injection vulnerability in browse.php in TriO 2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-31	7.5	CVE-2008-3418 MILW0RM
willo -- mobius_web_publishing_software	Multiple SQL injection vulnerabilities in Mobius Web Publishing Software 1.4.4.1 and earlier allow remote attackers to execute arbitrary SQL commands via (1) the id parameter to browse.php or (2) the s parameter in an exhibitions action to detail.php.	unknown 2008-07-31	7.5	CVE-2008-3420 MILW0RM BID
XMLSoft -- libxslt	Multiple heap-based buffer overflows in the rc4 (1) encryption (aka exsltCryptoRc4EncryptFunction) and (2) decryption (aka exsltCryptoRc4DecryptFunction) functions in crypto.c in libexslt in libxslt 1.1.8 through 1.1.24 allow context-dependent attackers to execute arbitrary code via an XML file containing a long string as "an argument in the XSL input."	unknown 2008-08-01	7.5	CVE-2008-2935 BUGTRAQ OTHER-REF BID

XOOPS -- Xoops	Directory traversal vulnerability in modules/system/admin.php in XOOPS 2.0.18 1 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the fct parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	7.5	CVE-2008-3296 BID XF
Youtube -- youtuber_clone	SQL injection vulnerability in ugroups.php in Youtuber Clone allows remote attackers to execute arbitrary SQL commands via the UID parameter.	unknown 2008-07-31	7.5	CVE-2008-3419 MILW0RM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
ATutor -- ATutor	PHP remote file inclusion vulnerability in tools/packages/import.php in ATutor 1.6.1 pl1 and earlier allows remote authenticated administrators to execute arbitrary PHP code via a URL in the type parameter.	unknown 2008-07-30	6.5	CVE-2008-3368 MILW0RM BID
avidweb_technologies -- jobbex_jobsite	search_result.cfm in Jobbex JobSite allows remote attackers to obtain sensitive information via unspecified vectors that reveal the installation path in an error message.	unknown 2008-07-28	6.8	CVE-2008-3339 BID XF
Blackboard -- Blackboard Academic Suite	Multiple cross-site request forgery (CSRF) vulnerabilities in Blackboard Academic Suite 8.0.260.7 allow remote attackers to change a student's configuration and enrollments via (1) update_module.jsp, (2) enroll_course.pl, and (3) unenroll.jsp.	unknown 2008-07-31	4.3	CVE-2008-3421 OTHER-REF SECTRACK XF
CalaCode -- atmail	Calacode @Mail 5.41 on Linux uses weak world-readable permissions for (1) webmail/libs/Atmail/Config.php and (2) webmail/webadmin/.htpasswd, which allows local users to obtain sensitive information by reading these files. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-31	5.0	CVE-2008-3395 BID
Carlos Desseno -- youtube_blog	Cross-site scripting (XSS) vulnerability in mensaje.php in C. Desseno YouTube Blog (ytb) 0.1 allows remote attackers to inject arbitrary web script or HTML via the m parameter.	unknown 2008-07-25	4.3	CVE-2008-3305 MILW0RM BID XF
Carlos Desseno -- youtube_blog	PHP remote file inclusion vulnerability in cuenta/cuerpo.php in C. Desseno YouTube Blog (ytb) 0.1, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the base_archivo parameter.	unknown 2008-07-25	6.8	CVE-2008-3308 MILW0RM BID XF
CMScout -- CMScout	Directory traversal vulnerability in common.php in CMScout 2.05, when .htaccess is not supported, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the bit parameter, as demonstrated by an upload to avatar/ of a .jpg file containing PHP sequences.	unknown 2008-07-31	6.4	CVE-2008-3415 MILW0RM BID
CoolPlayer -- CoolPlayer	Stack-based buffer overflow in CoolPlayer allows user-assisted remote attackers to execute arbitrary code via a crafted m3u file.	unknown 2008-07-31	6.8	CVE-2008-3408 MILW0RM BID
Edgewall Software -- Trac	Cross-site scripting (XSS) vulnerability in the wiki engine in Trac before 0.10.5 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	unknown 2008-07-27	4.3	CVE-2008-3328 OTHER-REF
Epic Games -- Unreal Tournament 2004	Unreal Tournament 2004 (UT2004) 3369 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a certain sequence of malformed packets.	unknown 2008-07-31	5.0	CVE-2008-3396 OTHER-REF OTHER-REF BID

Epic Games -- unreal_tournament_3	Unreal Tournament 3 1.3beta4 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a UDP packet in which the value of a certain size field is greater than the total packet length, aka attack 2 in ut3mendo.c.	unknown 2008-07-31	5.0	CVE-2008-3410 OTHER-REF OTHER-REF BID
fipsASP -- fipsCMS light	SQL injection vulnerability in home/index.asp in fipsCMS light 2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the r parameter, a different vector than CVE-2006-6115 and CVE-2007-2561.	unknown 2008-07-31	6.4	CVE-2008-3417 MILW0RM BID
GNU -- Coreutils	The default configuration of su in /etc/pam.d/su in GNU coreutils 5.2.1 allows local users to gain the privileges of a (1) locked or (2) expired account by entering the account name on the command line, related to improper use of the pam_succeed_if.so module.	unknown 2008-07-28	4.4	CVE-2008-1946 REDHAT BID SECTRACK
greatclone -- Auction Platinum	SQL injection vulnerability in category.php in Greatclone GC Auction Platinum allows remote attackers to execute arbitrary SQL commands via the cate_id parameter.	unknown 2008-07-31	6.4	CVE-2008-3413 MILW0RM
Grisoft -- AVG Antivirus	The files parsing engine in Grisoft AVG Anti-Virus before 8.0.156 allows remote attackers to cause a denial of service (engine crash) via a crafted UPX compressed file, which triggers a divide-by-zero error.	unknown 2008-07-30	5.0	CVE-2008-3373 OTHER-REF OTHER-REF BID
httrack -- winhttrack httrack -- httrack	Buffer overflow in URI processing in HTTrack and WinHTTrack before 3.42-3 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long URL.	unknown 2008-07-31	6.8	CVE-2008-3429 OTHER-REF OTHER-REF BID
infomining -- bookmine	Multiple cross-site scripting (XSS) vulnerabilities in search.cfm in BookMine allow remote attackers to inject arbitrary web script or HTML via the (1) gallery and (2) search_string parameters. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-31	4.3	CVE-2008-3394
jobbex -- jobsite	Cross-site scripting (XSS) vulnerability in search_result.cfm in Jobbex JobSite allows remote attackers to inject arbitrary web script or HTML via the searchFor variable (possibly the opt parameter.)	unknown 2008-07-28	4.3	CVE-2008-3340 BID XF
lemoncms -- lemon_cms	Directory traversal vulnerability in lemon_includes/FCKeditor/editor/filemanager/browser/browser.php in Lemon CMS 1.10 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the dir parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: this might be an issue in FCKeditor.	unknown 2008-07-25	6.8	CVE-2008-3312 OTHER-REF BID XF
linuxwebshop -- php_help_agent	Directory traversal vulnerability in include/head_chat.inc.php in php Help Agent 1.0 and 1.1 Full allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the content parameter. 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 2008-07-30	6.8	CVE-2008-3385 MILW0RM BID
mdsjack -- mjguest	Cross-site scripting (XSS) vulnerability in guestbook.js.php in MJGuest 6.8 GT allows remote attackers to inject arbitrary web script or HTML via the link parameter.	unknown 2008-07-31	4.3	CVE-2008-3404 BUGTRAQ BID
minishowcase -- minishowcase_image_gallery	Directory traversal vulnerability in libraries/general.init.php in Minishowcase Image Gallery 09b136, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter.	unknown 2008-07-31	6.8	CVE-2008-3390 BUGTRAQ MILW0RM XF
MoinMoin -- MoinMoin	Multiple cross-site scripting (XSS) vulnerabilities in macro/AdvancedSearch.py in moin (and MoinMoin) 1.6.3 and 1.7.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-07-30	4.3	CVE-2008-3381 OTHER-REF OTHER-REF OTHER-REF BID XF

Mono Project -- Mono	Multiple cross-site scripting (XSS) vulnerabilities in the ASP.net class libraries in Mono 2.0 and earlier allow remote attackers to inject arbitrary web script or HTML via crafted attributes related to (1) HtmlControl.cs (PreProcessRelativeReference), (2) HtmlForm.cs (RenderAttributes), (3) HtmlInputButton (RenderAttributes), (4) HtmlInputRadioButton (RenderAttributes), and (5) HtmlSelect (RenderChildren).	unknown 2008-07-31	4.3	CVE-2008-3422 OTHER-REF
MyioSoft -- easypublish	Cross-site scripting (XSS) vulnerability in staticpages/easypublish/index.php in MyioSoft EasyPublish 3.0tr allows remote attackers to inject arbitrary web script or HTML via the read parameter in an edp_News action.	unknown 2008-07-28	4.3	CVE-2008-3342 BUGTRAQ BID XF
MyioSoft -- easye-cards	Multiple cross-site scripting (XSS) vulnerabilities in staticpages/easyecards/index.php in MyioSoft EasyE-Cards 3.5 trial edition (tr) and 3.10a allow remote attackers to inject arbitrary web script or HTML via the (1) ResultHtml, (2) dir, (3) SenderName, (4) RecipientName, (5) SenderMail, and (6) RecipientMail parameters.	unknown 2008-07-28	4.3	CVE-2008-3344 BID XF
MyioSoft -- easye-cards	SQL injection vulnerability in staticpages/easyecards/index.php in MyioSoft EasyE-Cards 3.5 trial edition (tr) and 3.10a, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the sid parameter in a pickup action.	unknown 2008-07-28	6.8	CVE-2008-3345 BUGTRAQ BID XF
MyioSoft -- easydynamicpages	Cross-site scripting (XSS) vulnerability in staticpages/easycalendar/index.php in MyioSoft EasyDynamicPages 3.0 trial edition (tr) allows remote attackers to inject arbitrary web script or HTML via the year parameter.	unknown 2008-07-28	4.3	CVE-2008-3348 BUGTRAQ BID XF
MyioSoft -- easybookmarker	Cross-site scripting (XSS) vulnerability in ajaxp_backend.php in MyioSoft EasyBookMarker 4.0 trial edition (tr) allows remote attackers to inject arbitrary web script or HTML via the rs parameter.	unknown 2008-07-30	4.3	CVE-2008-3380 BUGTRAQ BID XF
nazgulled -- nzfotolog	Directory traversal vulnerability in index.php in Ricardo Amaral nzFotolog 0.4.1 allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the action_file parameter.	unknown 2008-07-31	6.8	CVE-2008-3405 MILW0RM BID XF
opensc-project -- opensc	OpenSC before 0.11.5 uses weak permissions (ADMIN file control information of 00) for the 5015 directory on smart cards and USB crypto tokens running Siemens CardOS M4, which allows physically proximate attackers to change the PIN.	unknown 2008-08-01	4.9	CVE-2008-2235 MLIST
Owl -- intranet_knowledgebase	Cross-site scripting (XSS) vulnerability in lib/owl.lib.php in Steve Bourgeois and Chris Vincent Owl Intranet Knowledgebase 0.95 and earlier allows remote attackers to inject arbitrary web script or HTML via the username parameter in a getpasswd action to register.php.	unknown 2008-07-29	4.3	CVE-2008-3100 BUGTRAQ
phpLinkat -- phpLinkat	phpLinkat 0.1 allows remote attackers to bypass authentication and access unspecified pages under admin/ by sending a login=right cookie.	unknown 2008-07-31	5.0	CVE-2008-3407 MILW0RM BID XF
puresw -- lore	Multiple cross-site scripting (XSS) vulnerabilities in Pure Software Lore before 1.7.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors related to the (1) article comments feature and the (2) search log feature.	unknown 2008-07-28	4.3	CVE-2008-3353 OTHER-REF
Python Software Foundation -- Python	Multiple integer overflows in the PyOS_vsnprintf function in Python/mysnprintf.c in Python 2.5.2 and earlier allow context-dependent attackers to cause a denial of service (memory corruption) or have unspecified other impact via crafted input to string formatting operations. NOTE: the handling of certain integer values is also affected by related integer underflows and an off-by-one error.	unknown 2008-08-01	5.0	CVE-2008-3144 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF GENTOO

runesoft -- cerberus_cms	Cross-site scripting (XSS) vulnerability in Runesoft Cerberus CMS before 3_1.4_0.9 allows remote attackers to inject arbitrary web script or HTML via a cerberus_user cookie.	unknown 2008-07-31	4.3	CVE-2008-3397 OTHER-REF BID
SAP -- MaxDB	Untrusted search path vulnerability in dbmsrv in SAP MaxDB 7.6.03.15 on Linux allows local users to gain privileges via a modified PATH environment variable.	unknown 2008-08-01	4.4	CVE-2008-1810 IDEFENSE
SiteAdmin -- CMS	SQL injection vulnerability in line2.php in SiteAdmin allows remote attackers to execute arbitrary SQL commands via the art parameter.	unknown 2008-07-31	6.4	CVE-2008-3414 MILW0RM SECUNIA
snarky -- visualpic	Cross-site scripting (XSS) vulnerability in Snark VisualPic 0.3.1 allows remote attackers to inject arbitrary web script or HTML via the pic parameter to the default URI. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-30	4.3	CVE-2008-3379 BID XF
Social Engine -- Social Engine	SocialEngine (SE) before 2.83 grants certain write privileges for templates, which allows remote authenticated administrators to execute arbitrary PHP code.	unknown 2008-07-25	6.0	CVE-2008-3298 BUGTRAQ XF
Sun -- Java System Web Server plugin Sun -- N1 Service Provisioning System	Unspecified vulnerability in the Sun Java System Web Server 7.0 plugin in Sun N1 Service Provisioning System (SPS) 5.2 and 6.0 allows remote authenticated SPS users to gain administrative access to the web server via unknown attack vectors.	unknown 2008-07-31	6.5	CVE-2008-3425 SUNALERT BID
the_kelleys -- dnsmasq	dnsmasq 2.43 allows remote attackers to cause a denial of service (daemon crash) by (1) sending a DHCPINFORM while lacking a DHCP lease, or (2) attempting to renew a nonexistent DHCP lease for an invalid subnet as an "unknown client," a different vulnerability than CVE-2008-3214.	unknown 2008-07-28	5.0	CVE-2008-3350 OTHER-REF
tuxplanet -- bilboblog	SQL injection vulnerability in admin/delete.php in BilboBlog 0.2.1, when magic_quotes_gpc is disabled, allows remote authenticated administrators to execute arbitrary SQL commands via the num parameter.	unknown 2008-07-25	6.0	CVE-2008-3302 MILW0RM XF
tuxplanet -- bilboblog	admin/login.php in BilboBlog 0.2.1, when register_globals is enabled, allows remote attackers to bypass authentication and obtain administrative access via a direct request that sets the login, admin_login, password, and admin_passwd parameters.	unknown 2008-07-25	6.8	CVE-2008-3303 MILW0RM BID XF
tuxplanet -- bilboblog	BilboBlog 0.2.1 allows remote attackers to obtain sensitive information via (1) an enable_cache=false query string to footer.php or (2) a direct request to pagination.php, which reveals the installation path in an error message.	unknown 2008-07-25	5.0	CVE-2008-3304 MILW0RM XF
webwizguide -- web_wiz_rich_text_editor	Cross-site scripting (XSS) vulnerability in RTE_popup_link.asp in Web Wiz Rich Text Editor (RTE) 3.x and 4.x before 4.03 allows remote attackers to inject arbitrary web script or HTML via the email parameter.	unknown 2008-07-30	4.3	CVE-2008-3367 BUGTRAQ OTHER-REF BID
webwizguide -- web_wiz_forums	Multiple cross-site scripting (XSS) vulnerabilities in Web Wiz Forum 9.5 allow remote attackers to inject arbitrary web script or HTML via the mode parameter to (1) admin_group_details.asp and (2) admin_category_details.asp.	unknown 2008-07-31	4.3	CVE-2008-3391 OTHER-REF OTHER-REF BID XF
webwizguide -- web_wiz_forums	Cross-site request forgery (CSRF) vulnerability in Web Wiz Forum 9.5 allows remote attackers to log out a user via a link or IMG tag to log_off_user.asp.	unknown 2008-07-31	5.8	CVE-2008-3392 OTHER-REF XF
XOOPS -- Xoops	Cross-site scripting (XSS) vulnerability in modules/system/admin.php in XOOPS 2.0.18.1 allows remote attackers to inject arbitrary web script or HTML via the fct parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-25	4.3	CVE-2008-3295 BID XF

xrms -- xrms_crm	PHP remote file inclusion vulnerability in activities/workflow-activities.php in XRMS CRM 1.99.2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the include_directory parameter.	unknown 2008-07-31	4.3	CVE-2008-3399 BUGTRAQ MILW0RM XF
xrms -- xrms_crm	XRMS CRM 1.99.2 allows remote attackers to obtain configuration information via a direct request to tests/info.php, which calls the phpinfo function.	unknown 2008-07-31	4.3	CVE-2008-3400 BUGTRAQ MILW0RM
Zdaemon -- Zdaemon	ZDaemon 1.08.07 and earlier allows remote attackers to cause a denial of service (daemon crash) via a crafted type 6 command, which triggers a NULL pointer dereference.	unknown 2008-07-25	5.0	CVE-2008-3314 BUGTRAQ OTHER-REF OTHER-REF BID XF

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Moodle -- Moodle	Cross-site scripting (XSS) vulnerability in blog/edit.php in Moodle 1.6.x before 1.6.7 and 1.7.x before 1.7.5 allows remote attackers to inject arbitrary web script or HTML via the etitle parameter (blog entry title).	unknown 2008-07-25	2.6	CVE-2008-3326 OTHER-REF OTHER-REF
phpFreeChat -- phpFreeChat	Session fixation vulnerability in phpFreeChat 1.1 allows remote authenticated users to hijack web sessions by setting the session_id parameter to match the victim's nickid parameter.	unknown 2008-07-31	0.0	CVE-2008-3428
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in the Solaris Platform Information and Control Library daemon (picld) in Sun Solaris 8 through 10, and OpenSolaris builds snv_01 through snv_95, allows local users to cause a denial of service via unknown vectors that prevent operation of utilities such as prtdiag, prtpicl, and prtfru.	unknown 2008-07-31	2.1	CVE-2008-3426 SUNALERT BID
tuxplanet -- bilboblog	Multiple cross-site scripting (XSS) vulnerabilities in BilboBlog 0.2.1 allow remote authenticated administrators to inject arbitrary web script or HTML via the (1) content parameter to admin/update.php, related to conflicting code in widget.php; and allow remote attackers to inject arbitrary web script or HTML via the (2) titleId parameter to head.php, reachable through index.php; the (3) t_lang[lang_copyright] parameter to footer.php; the (4) content parameter to the default URI under admin/; the (5) url, (6) t_lang[lang_admin_help], (7) t_lang[lang_admin_clear_cache], (8) t_lang[lang_admin_home], and (9) t_lang[lang_admin_logout] parameters to admin/homelink.php; and the (10) t_lang[lang_admin_new_post] parameter to admin/post.php. NOTE: some of these details are obtained from third party information.	unknown 2008-07-25	3.5	CVE-2008-3301 MILW0RM BID XF
xrms -- xrms_crm	Multiple cross-site scripting (XSS) vulnerabilities in XRMS CRM 1.99.2 allow remote attackers to inject arbitrary web script or HTML via the msg parameter to unspecified components, possibly including login.php. NOTE: this may overlap CVE-2008-1129.	unknown 2008-07-31	2.6	CVE-2008-3398 BUGTRAQ MILW0RM BID XF

Back to top