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
benjacms -- benja_cms	Unrestricted file upload vulnerability in admin/upload.php in Benja CMS 0.1 allows remote attackers to upload and execute arbitrary PHP files via unspecified vectors, followed by a direct request to the file in billeder/.	unknown 2008-07-02	7.5	CVE-2008-2988 BUGTRAQ BID XF
cartweaver -- cartweaver	SQL injection vulnerability in details.php in Application Dynamics Cartweaver 3.0 allows remote attackers to execute arbitrary SQL commands via the prodId parameter, possibly a related issue to CVE-2006-2046.3.	unknown 2008-06-30	7.5	CVE-2008-2918 MILW0RM BID
CiStyle -- ciblog	SQL injection vulnerability in links-extern.php in CiBlog 3.1 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-02	7.5	CVE-2008-2971 MILW0RM BID XF

cmsmini -- cms_mini	Multiple directory traversal vulnerabilities in view/index.php in CMS Mini 0.2.2 allow remote attackers to read arbitrary local files via a .. (dot dot) in the (1) path and (2) p parameter.	unknown 2008-07-02	7.5	CVE-2008-2961 MILW0RM BID XF
CWH Underground -- demo4_cms	SQL injection vulnerability in index.php in Demo4 CMS 01 Beta allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-02	7.5	CVE-2008-2983 MILW0RM XF
Drupal -- Drupal Drupal -- aggregation_module	Multiple SQL injection vulnerabilities in the Aggregation module 5.x before 5.x-4.4 for Drupal allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2008-07-03	7.5	CVE-2008-2999
Drupal -- Drupal Drupal -- aggregation_module	The Aggregation module 5.x before 5.x-4.4 for Drupal allows remote attackers to upload files with arbitrary extensions, and possibly execute arbitrary code, via a crafted feed that allows upload of files with arbitrary extensions.	unknown 2008-07-03	9.3	CVE-2008-3001
ezcms -- eztechhelp_ezcms	admin/filemanager/ (aka the File Manager) in EZTechhelp EZCMS 1.2 and earlier does not require authentication, which allows remote attackers to create, modify, read, and delete files.	unknown 2008-06-30	7.5	CVE-2008-2920 MILW0RM
EZTechhelp Company -- EZCMS	SQL injection vulnerability in index.php in EZTechhelp EZCMS 1.2 and earlier allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2008-06-30	7.5	CVE-2008-2921 MILW0RM BID
fog -- fog_forum	Multiple directory traversal vulnerabilities in index.php in FOG Forum 0.8.1 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) fog_lang and (2) fog_skin parameters, probably related to libs/required/share.inc; and possibly the (3) fog_pseudo, (4) fog_posted, (5) fog_password, and (6) fog_cook parameters.	unknown 2008-07-03	7.5	CVE-2008-2993 MILW0RM BID

homap -- homap	SQL injection vulnerability in index.php in HoMaP-CMS 0.1 allows remote attackers to execute arbitrary SQL commands via the go parameter.	unknown 2008-07-02	7.5	CVE-2008-2989 MILW0RM BID XF
JaxUltraBB -- JaxUltraBB	Directory traversal vulnerability in viewprofile.php in JaxUltraBB 2.0 and earlier allows remote attackers to read arbitrary local files via a .. (dot dot) in the user parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-02	7.5	CVE-2008-2966 BID XF
Joomla -- com_facileforms Mambo -- com_facileforms Joomla -- Joomla	PHP remote file inclusion vulnerability in facileforms.frame.php in the FacileForms (com_facileforms) component 1.4.4 for Mambo and Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the ff_compath parameter.	unknown 2008-07-02	7.5	CVE-2008-2990 MILW0RM BID XF
kblance.com -- php_knowledgebase_script kblance.com -- kblance.com	SQL injection vulnerability in index.php in KbLance allows remote attackers to execute arbitrary SQL commands via the cat_id parameter in a comment action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-02	7.5	CVE-2008-2972 BID XF
Linux -- direct_connect	client/NmdcHub.cpp in Linux DC++ (linuxdcpp) before 0.707 allows remote attackers to cause a denial of service (crash) via an empty private message, which triggers an out-of-bounds read.	unknown 2008-07-01	7.8	CVE-2008-2954 OTHER-REF OTHER-REF
Microsoft -- Visual Basic Enterprise Edition	Buffer overflow in a certain ActiveX control (vb6skit.dll) in Microsoft Visual Basic Enterprise Edition 6.0 SP6 might allow remote attackers to execute arbitrary code via a long lpstrLinkPath argument to the fCreateShellLink function.	unknown 2008-07-02	9.3	CVE-2008-2959 MILW0RM BID XF
ourvideo_cms -- ourvideo_cms	Multiple PHP remote file inclusion vulnerabilities in Ourvideo CMS 9.5 allow remote attackers to execute arbitrary PHP code via a URL in the include_connection parameter to (1) edit_top_feature.php and (2) edit_topics_feature.php in phpi/.	unknown 2008-07-02	7.5	CVE-2008-2977 MILW0RM BID

phpdmca -- phpdmca	Multiple PHP remote file inclusion vulnerabilities in phpDMCA 1.0.0 allow remote attackers to execute arbitrary PHP code via a URL in the ourlinux_root_path parameter to (1) adodb-errorpear.inc.php and (2) adodb-pear.inc.php in adodb/.	unknown 2008-07-02	7.5	CVE-2008-2986 MILW0RM BID XF
phpeasydata -- phpeasydata	Multiple SQL injection vulnerabilities in PHPEasyData 1.5.4 allow remote attackers to execute arbitrary SQL commands via (1) the annuaire parameter to annuaire.php or (2) the username field in admin/login.php.	unknown 2008-07-03	7.5	CVE-2008-2995 BUGTRAQ BID
researchguide -- researchguide	SQL injection vulnerability in guide.php in ResearchGuide 0.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-07-02	7.5	CVE-2008-2964 MILW0RM XF
Sun -- Java System Access Manager Sun -- java_system_identity_server	Sun Java System Access Manager 6.3 through 7.1 and Sun Java System Identity Server 6.1 and 6.2 do not properly process XSLT stylesheets in XSLT transforms in XML signatures, which allows context-dependent attackers to execute arbitrary code via a crafted stylesheet, a related issue to CVE-2007-3715, CVE-2007-3716, and CVE-2007-4289.	unknown 2008-06-30	7.5	CVE-2008-2945 SUNALERT
Sun -- Solaris	The SNMP-DMI mapper subagent daemon (aka snmpXdmid) in Solstice Enterprise Agents in Sun Solaris 8 through 10 allows remote attackers to cause a denial of service (daemon crash) via malformed packets.	unknown 2008-06-30	7.8	CVE-2008-2946 SUNALERT BID
t0pP8uZz -- Dana IRC Client	Stack-based buffer overflow in artegic Dana IRC client 1.3 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long IRC message.	unknown 2008-06-30	7.5	CVE-2008-2922 MILW0RM BID
Valarsoft -- WebMatic	SQL injection vulnerability in Webmatic before 2.8 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	unknown 2008-06-30	7.5	CVE-2008-2925
yektaweb -- academic_web_tools	SQL injection vulnerability in rating.php in Academic Web Tools	unknown 2008-07-02	7.5	CVE-2008-2968 BUGTRAQ

	(AWT YEKTA) 1.4.3.1, and 1.4.2.8 and earlier, allows remote attackers to execute arbitrary SQL commands via the book_id parameter.			OTHER-REF BID XF
yektaweb -- academic_web_tools	Multiple session fixation vulnerabilities in Academic Web Tools (AWT YEKTA) 1.4.3.1, and 1.4.2.8 and earlier, allow remote attackers to hijack web sessions by setting the PHPSESSID parameter to (1) index.php and (2) login.php in homepg/.	unknown 2008-07-02	7.5	CVE-2008-2970 BUGTRAQ OTHER-REF BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Apple -- Mac OS X Server Apple -- Mac OS X	Unspecified vulnerability in Alias Manager in Apple Mac OS X 10.5.1 and earlier on Intel platforms allows local users to gain privileges or cause a denial of service (memory corruption and application crash) by resolving an alias that contains crafted AFP volume mount information.	unknown 2008-07-01	4.6	CVE-2008-2308 OTHER-REF APPLE BID SECTRACK
Apple -- Mac OS X Server Apple -- Mac OS X	Incomplete blacklist vulnerability in CoreTypes in Apple Mac OS X before 10.5.4 allows user-assisted remote attackers to execute arbitrary code via a (1) .xht or (2) .xhtm file, which does not trigger a "potentially unsafe" warning message in (a) the Download Validation feature in Mac OS X 10.4 or (b) the Quarantine feature in Mac OS X 10.5.	unknown 2008-07-01	6.8	CVE-2008-2309 OTHER-REF APPLE BID SECTRACK
Apple -- Mac OS X Server Apple -- Mac OS X	Format string vulnerability in c++filt in Apple Mac OS X 10.5 before 10.5.4 allows user-assisted attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted string in (1) C++ or (2) Java source code.	unknown 2008-07-01	6.8	CVE-2008-2310 OTHER-REF APPLE BID SECTRACK
Apple -- Mac OS X Server Apple -- Mac OS X	Launch Services in Apple Mac OS X before 10.5, when Open Safe Files is enabled, allows remote attackers to execute arbitrary code via a symlink attack, probably related to a race condition and automatic execution of a downloaded file.	unknown 2008-07-01	6.8	CVE-2008-2311 OTHER-REF APPLE BID SECTRACK

Apple -- Mac OS X Server Apple -- Mac OS X	Apple Mac OS X before 10.5 uses weak permissions for the User Template directory, which allows local users to gain privileges by inserting a Trojan horse file into this directory.	unknown 2008-07-01	4.6	CVE-2008-2313 OTHER-REF APPLE BID SECTRACK
Apple -- Mac OS X Server Apple -- Mac OS X	Dock in Apple Mac OS X 10.5 before 10.5.4, when Exposé hot corners is enabled, allows physically proximate attackers to gain access to a locked session in (1) sleep mode or (2) screen saver mode via unspecified vectors.	unknown 2008-07-01	4.4	CVE-2008-2314 OTHER-REF APPLE BID SECTRACK
benjacms -- benja_cms	Multiple cross-site scripting (XSS) vulnerabilities in Benja CMS 0.1 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) admin_edit_submenu.php, (2) admin_new_submenu.php, and (3) admin_edit_topmenu.php in admin/.	unknown 2008-07-02	4.3	CVE-2008-2987 BUGTRAQ BID XF
caucho -- resin	Cross-site scripting (XSS) vulnerability in the viewfile documentation command in Caucho Resin before 3.0.25, and 3.1.x before 3.1.4, allows remote attackers to inject arbitrary web script or HTML via the file parameter.	unknown 2008-06-30	4.3	CVE-2008-2462 OTHER-REF CERT-VN BID XF
checkinstall -- checkinstall	Race condition in (1) checkinstall 1.6.1 and (2) installwatch allows local users to overwrite arbitrary files and have other impacts via symlink and possibly other attacks on temporary working directories.	unknown 2008-07-01	4.4	CVE-2008-2958 OTHER-REF OTHER-REF XF
cmreams -- cmreams_cms	Cross-site scripting (XSS) vulnerability in backend/umleitung.php in CMReams CMS 1.3.1.1 Beta 2 allows remote attackers to inject arbitrary web script or HTML via the lang[be_red_text] parameter.	unknown 2008-07-02	4.3	CVE-2008-2984 MILW0RM BID XF
cmreams -- cmreams_cms	Directory traversal vulnerability in load_language.php in CMReams CMS 1.3.1.1 Beta 2, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the page_language parameter.	unknown 2008-07-02	6.8	CVE-2008-2985 MILW0RM BID XF
Drupal -- Drupal Drupal -- aggregation_module	Multiple cross-site scripting (XSS) vulnerabilities in the Aggregation module 5.x before 5.x-4.4 for Drupal allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-07-03	4.3	CVE-2008-2998
Drupal -- Drupal Drupal -- aggregation_module	The Aggregation module 5.x before 5.x-4.4 for Drupal, when node access modules are used, does not properly implement access control,	unknown 2008-07-03	6.8	CVE-2008-3000

	which allows remote attackers to bypass intended restrictions.			
gravityboardx -- gravity_board_x	Multiple SQL injection vulnerabilities in index.php in Gravity Board X (GBX) 2.0 Beta, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) searchquery parameter in a getsearch action, and the (2) board_id parameter in a viewboard action.	unknown 2008-07-03	6.8	CVE-2008-2996 MILW0RM BID XF
gravityboardx -- gravity_board_x	Cross-site scripting (XSS) vulnerability in index.php in Gravity Board X (GBX) 2.0 Beta allows remote attackers to inject arbitrary web script or HTML via the subject parameter in a postnewsubmit (aka create new thread) action.	unknown 2008-07-03	4.3	CVE-2008-2997 MILW0RM BID XF
gryphonllc -- gryphon_gllcts2	SQL injection vulnerability in listing.php in Gryphon gllcTS2 4.2.4 allows remote attackers to execute arbitrary SQL commands via the sort parameter.	unknown 2008-06-30	6.8	CVE-2008-2919 MILW0RM BID
homeph_design -- homeph_design	Multiple cross-site scripting (XSS) vulnerabilities in HomePH Design 2.10 RC2 allow remote attackers to inject arbitrary web script or HTML via the (1) error_meldung parameter to admin/features/register/register.php, the (2) feature_language[ueberschrift] parameter to admin/features/memberlist/memberlist.php, the (3) language_array[ueberschrift] parameter to admin/features/lostpassword/lostpassword.php, the (4) language_feature[titel] parameter to admin/features/kalender/eingabe.php, and the (5) language_feature[bildmenu] parameter to admin/features/fotogalerie/eingabe.php.	unknown 2008-07-02	4.3	CVE-2008-2980 MILW0RM XF
homeph_design -- homeph_design	PHP remote file inclusion vulnerability in admin/templates/template_thumbnail.php in HomePH Design 2.10 RC2, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the thumb_template parameter.	unknown 2008-07-02	6.8	CVE-2008-2981 MILW0RM XF
homeph_design -- homeph_design	Multiple directory traversal vulnerabilities in HomePH Design 2.10 RC2, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the (1) thumb_template parameter to (a) admin/templates/template_thumbnail.php, and the (2) language parameter to (b)	unknown 2008-07-02	6.8	CVE-2008-2982 MILW0RM XF

	account/account.php, (c) downloads/downloads.php, (d) forum/forum.php, (e) fotogalerie/delete.php, and (f) fotogalerie/fotogalerie.php in admin/features/.			
IBM -- Tivoli Directory Server	Double free vulnerability in IBM Tivoli Directory Server (TDS) 6.1.0.0 through 6.1.0.15 allows remote authenticated administrators to cause a denial of service (ABEND) and possibly execute arbitrary code by using ldapadd to attempt to create a duplicate ibm-globalAdminGroup LDAP database entry. NOTE: the vendor states "There is no real risk of a vulnerability," although there are likely scenarios in which a user is allowed to make administrative LDAP requests but does not have the privileges to stop the server.	unknown 2008-06-30	6.0	CVE-2008-2943 AIXAPAR
jaxbot -- jaxultrabb	Cross-site scripting (XSS) vulnerability in viewforum.php in JaxUltraBB (JUBB) 2.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the forum parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-07-02	4.3	CVE-2008-2965 BID XF
kernel -- linux	The Linux kernel 2.6.24 and 2.6.25 before 2.6.25.9 allows local users to cause a denial of service (memory consumption) via a large number of calls to the get_user_pages function, which lacks a ZERO_PAGE optimization and results in allocation of "useless newly zeroed pages."	unknown 2008-07-02	4.9	CVE-2008-2372 MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF
kernel -- linux	Integer overflow in the sctp_getsockopt_local_addrs_old function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) functionality in the Linux kernel before 2.6.25.9 allows local users to cause a denial of service (resource consumption and system outage) via vectors involving a large addr_num field in an sctp_getaddrs_old data structure.	unknown 2008-07-02	4.9	CVE-2008-2826 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
Linux -- Kernel	Unspecified vulnerability in the 32-bit and 64-bit emulation in the Linux kernel 2.6.9, 2.6.18, and probably other versions allows local users to read uninitialized memory via unknown vectors involving a crafted binary.	unknown 2008-06-30	4.9	CVE-2008-0598 OTHER-REF REDHAT REDHAT

Linux -- direct connect	Linux DC++ (linuxdcpp) before 0.707 allows remote attackers to cause a denial of service (crash) via "partial file list requests" that trigger a NULL pointer dereference.	unknown 2008-07-01	5.0	CVE-2008-2953 OTHER-REF OTHER-REF
Lyris -- List Manager	Cross-site scripting (XSS) vulnerability in read/search/results in Lyris ListManager 8.8, 8.95, and 9.3d allows remote attackers to inject arbitrary web script or HTML via the words parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-30	4.3	CVE-2008-2923
Mercurial -- Mercurial	Directory traversal vulnerability in patch.py in Mercurial 1.0.1 allows user-assisted attackers to modify arbitrary files via ".." (dot dot) sequences in a patch file.	unknown 2008-06-30	6.8	CVE-2008-2942 OTHER-REF MLIST
Microsoft -- Internet Explorer	Cross-domain vulnerability in Microsoft Internet Explorer 6 allows remote attackers to access restricted information from other domains via JavaScript that uses the Object data type for the value of a (1) location or (2) location.href property.	unknown 2008-06-30	6.8	CVE-2008-2947 OTHER-REF OTHER-REF CERT-VN BID XF
Microsoft -- Internet Explorer	Cross-domain vulnerability in Microsoft Internet Explorer 7 and 8 allows remote attackers to change the location property of a frame via the Object data type, and use a frame from a different domain to observe domain-independent events, as demonstrated by observing onkeydown events with caballero-listener.	unknown 2008-06-30	6.8	CVE-2008-2948 OTHER-REF OTHER-REF OTHER-REF OTHER-REF CERT-VN
Microsoft -- Internet Explorer	Cross-domain vulnerability in Microsoft Internet Explorer 6 and 7 allows remote attackers to change the location property of a frame via the String data type, and use a frame from a different domain to observe domain-independent events, as demonstrated by observing onkeydown events with caballero-listener.	unknown 2008-06-30	6.8	CVE-2008-2949 OTHER-REF OTHER-REF OTHER-REF CERT-VN
mm_chat -- mm_chat	Multiple cross-site scripting (XSS) vulnerabilities in chathead.php in MM Chat 1.5 allow remote attackers to inject arbitrary web script or HTML via the (1) sitename and (2) wmessage parameters.	unknown 2008-07-02	4.3	CVE-2008-2973 MILW0RM BID
mm_chat -- mm_chat	Directory traversal vulnerability in chatconfig.php in MM Chat 1.5, when register_globals is enabled, allows remote attackers to include and execute arbitrary local	unknown 2008-07-02	6.8	CVE-2008-2974 MILW0RM BID

	files via directory traversal sequences in the currentlang parameter.			
MyBlog -- MyBlog	Multiple cross-site scripting (XSS) vulnerabilities in MyBlog allow remote attackers to inject arbitrary web script or HTML via the (1) s and (2) sort parameters to index.php, and the (3) id parameter to post.php.	unknown 2008-07-02	4.3	CVE-2008-2962 MILW0RM BID
MyBlog -- MyBlog	Multiple SQL injection vulnerabilities in MyBlog allow remote attackers to execute arbitrary SQL commands via the (1) view parameter to (a) index.php, and the (2) id parameter to (b) member.php and (c) post.php.	unknown 2008-07-02	6.8	CVE-2008-2963 MILW0RM BID XF
OpenLDAP -- OpenLDAP	liblber/io.c in OpenLDAP 2.3.41, 2.3.42, and possibly other versions allows remote attackers to cause a denial of service (program termination) via crafted ASN.1 BER datagrams, which triggers an assertion error.	unknown 2008-07-01	5.0	CVE-2008-2952 OTHER-REF
ourvideo_cms -- ourvideo_cms	Multiple cross-site scripting (XSS) vulnerabilities in phpi/login.php in Ourvideo CMS 9.5 allow remote attackers to inject arbitrary web script or HTML via the (1) top_page and (2) end_page parameters.	unknown 2008-07-02	4.3	CVE-2008-2979 MILW0RM BID
ourvideocms -- ourvideo_cms	Directory traversal vulnerability in phpi/rss.php in Ourvideo CMS 9.5, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the prefix parameter.	unknown 2008-07-02	6.8	CVE-2008-2978 MILW0RM BID
phpeasydata -- phpeasydata	Multiple cross-site scripting (XSS) vulnerabilities in PHPEasyData 1.5.4 allow remote attackers to inject arbitrary web script or HTML via the (1) annuaire parameter to (a) last_records.php and (b) annuaire.php and the (2) by and (3) cat_id parameters to annuaire.php.	unknown 2008-07-03	4.3	CVE-2008-2994 BUGTRAQ BID XF
phpMyAdmin -- phpMyAdmin	Cross-site scripting (XSS) vulnerability in phpMyAdmin before 2.11.7, when register_globals is enabled and .htaccess support is disabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving scripts in libraries/.	unknown 2008-07-02	4.3	CVE-2008-2960 OTHER-REF
Pidgin -- Pidgin	Pidgin 2.4.1 allows remote attackers to cause a denial of service (crash) via a long filename that contains certain characters, as	unknown 2008-07-01	4.3	CVE-2008-2955 BUGTRAQ

	demonstrated using an MSN message that triggers the crash in the msn_slplink_process_msg function.			
Pidgin -- Pidgin	Memory leak in Pidgin 2.0.0, and possibly other versions, allows remote attackers to cause a denial of service (memory consumption) via malformed XML documents.	unknown 2008-07-01	5.0	CVE-2008-2956 OTHER-REF MLIST BID
Pidgin -- Pidgin	The UPnP functionality in Pidgin 2.0.0, and possibly other versions, allows remote attackers to trigger the download of arbitrary files and cause a denial of service (memory or disk consumption) via a UDP packet that specifies an arbitrary URL.	unknown 2008-07-01	6.4	CVE-2008-2957 OTHER-REF MLIST BID
Red Hat -- Desktop Red Hat -- Enterprise Linux WS Red Hat -- Enterprise Linux ES Linux -- Kernel Red Hat -- Enterprise Linux AS	Race condition in the ptrace and utrace support in the Linux kernel 2.6.9 through 2.6.25, as used in Red Hat Enterprise Linux (RHEL) 4, allows local users to cause a denial of service (oops) via a long series of PTRACE_ATTACH ptrace calls to another user's process that trigger a conflict between utrace_detach and report_quiescent, related to "late ptrace_may_attach() check" and "race around &dead_engine_ops setting," a different vulnerability than CVE-2007-0771 and CVE-2008-1514.	unknown 2008-06-30	4.7	CVE-2008-2365 MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
Red Hat -- linux kernel	arch/x86_64/lib/copy_user.S in the Linux kernel before 2.6.19 on some AMD64 systems does not erase destination memory locations after an exception during kernel memory copy, which allows local users to obtain sensitive information.	unknown 2008-06-30	4.9	CVE-2008-2729 OTHER-REF OTHER-REF REDHAT REDHAT
Red Hat -- enterprise linux kernel Red Hat -- fedora core	Double free vulnerability in the utrace support in the Linux kernel, probably 2.6.18, in Red Hat Enterprise Linux (RHEL) 5 and Fedora Core 6 (FC6) allows local users to cause a denial of service (oops), as demonstrated by a crash when running the GNU GDB testsuite, a different vulnerability than CVE-2008-2365.	unknown 2008-06-30	4.9	CVE-2008-2944 OTHER-REF OTHER-REF
tinx_cms -- tinx_cms	Cross-site scripting (XSS) vulnerability in admin/objects/obj_image.php in TinX/cms 1.1 allows remote attackers to inject arbitrary web script or HTML via the language parameter.	unknown 2008-07-02	4.3	CVE-2008-2975 MILW0RM BID XF
tinx_cms -- tinx_cms	Multiple directory traversal vulnerabilities in TinX/cms 1.1, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via directory	unknown 2008-07-02	6.8	CVE-2008-2976 MILW0RM BID

	traversal sequences in the (1) language parameter to (a) include_me.php, (b) admin/ajax.php, and (c) admin/objects/catalog.ajaxhandler.php; and the (2) prefix parameter to (d) admin/inc/config.php.			
Valarsoft -- WebMatic	Cross-site scripting (XSS) vulnerability in Webmatic before 2.8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-30	4.3	CVE-2008-2924
yektaweb -- academic_web_tools	Multiple cross-site scripting (XSS) vulnerabilities in Academic Web Tools (AWT YEKTA) 1.4.3.1, and 1.4.2.8 and earlier, allow remote attackers to inject arbitrary web script or HTML via the (1) query string to login.php and the (2) glb_sid parameter to hta/htmlarea.js.php, and allow remote authenticated users to inject arbitrary web script or HTML via an unspecified field in room.php.	unknown 2008-07-02	4.3	CVE-2008-2967 BUGTRAQ OTHER-REF BID XF
yektaweb -- academic_web_tools	Directory traversal vulnerability in download.php in Academic Web Tools (AWT YEKTA) 1.4.3.1, and 1.4.2.8 and earlier, allows remote attackers to read arbitrary files via a .. (dot dot) in the dfile parameter.	unknown 2008-07-02	5.0	CVE-2008-2969 BUGTRAQ OTHER-REF BID XF

Back to top

There were no low vulnerabilities recorded this week.