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
Avaya -- Communication Manager Avaya -- SIP Enablement Services	The remote management interface in SIP Enablement Services (SES) Server in Avaya SIP Enablement Services 5.0, and Communication Manager (CM) 5.0 on the S8300C with SES enabled, proceeds with Core router updates even when a login is invalid, which allows remote attackers to cause a denial of service (messaging outage) or gain privileges via an update request.	unknown 2008-08-25	7.5	CVE-2008-3778 OTHER-REF BID XF
btiteam -- xbtitracker btiteam -- btitracker	SQL injection vulnerability in scrape.php in BtiTracker 1.4.7 and earlier and xBtiTracker 2.0.542 and earlier allows remote attackers to execute arbitrary SQL commands via the info_hash parameter.	unknown 2008-08-26	7.5	CVE-2008-3784 MILW0RM BID
craftysyntax -- crafty_syntax_live_help	Multiple SQL injection vulnerabilities in Crafty Syntax Live	unknown	7.5	CVE-2008-3845 BUGTRAQ

	Help (CSLH) 2.14.6 and earlier allow remote attackers to execute arbitrary SQL commands via the department parameter to (1) is_xmlhttp.php and (2) is_flush.php.	2008-08-27		MILW0RM OTHER-REF OTHER-REF BID
IBM -- DB2 Universal Database	Unspecified vulnerability in the CLR stored procedure deployment from IBM Database Add-Ins for Visual Studio in the Visual Studio Net component in IBM DB2 9.1 before Fixpak 5 has unknown impact and attack vectors.	unknown 2008-08-28	7.5	CVE-2008-3852 OTHER-REF AIXAPAR BID
IBM -- DB2 Universal Database	Buffer overflow in the DAS server program in the Core DAS function component in IBM DB2 9.1 before Fixpak 4a allows remote attackers to execute arbitrary code or cause a denial of service (daemon crash) via unspecified vectors. NOTE: this might be related to CVE-2008-0698.	unknown 2008-08-28	9.3	CVE-2008-3853
IBM -- DB2 Universal Database	Multiple stack-based buffer overflows in IBM DB2 9.1 before Fixpak 5 allow remote attackers to cause a denial of service (system outage) via vectors related to (1) use of XQuery to issue statements; the (2) XMLQUERY, (3) XMLEXISTS, and (4) XMLTABLE statements; and the (5) sqlrlaka function.	unknown 2008-08-28	7.8	CVE-2008-3854
IBM -- DB2 Universal Database	The routine infrastructure component in IBM DB2 9.1 before Fixpak 5 on Unix and Linux does not change the ownership of the db2fmp process, which has unknown impact and attack vectors.	unknown 2008-08-28	7.5	CVE-2008-3856
Ipswitch -- ws_ftp_home	Buffer overflow in Ipswitch WS_FTP Home client allows remote FTP servers to have an unknown impact via a long "message response."	unknown 2008-08-27	10.0	CVE-2008-3795 MILW0RM
libTIFF -- libTIFF	Multiple buffer underflows in the (1) LZWDecode and (2) LZWDecodeCompat functions in tif_lzw.c in the LZW decoder in LibTIFF 3.8.2 and earlier allow context-dependent attackers to	unknown 2008-08-27	7.5	CVE-2008-2327 OTHER-REF OTHER-REF OTHER-REF BID

	execute arbitrary code via a crafted TIFF file. NOTE: some of these details are obtained from third party information.			
Linux -- Kernel	Integer overflow in the sctp_setsockopt_auth_key function in net/sctp/socket.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel 2.6.24-rc1 through 2.6.26.3 allows remote attackers to cause a denial of service (panic) or possibly have unspecified other impact via a crafted sca_keylength field associated with the SCTP_AUTH_KEY option.	unknown 2008-08-27	7.8	CVE-2008-3526 MLIST OTHER-REF BID
miacms -- miacms miacms -- com_component	Multiple SQL injection vulnerabilities in the com_content component in MiaCMS 4.6.5 allow remote attackers to execute arbitrary SQL commands via the id parameter in a (1) view, (2) category, or (3) blogsection action to index.php.	unknown 2008-08-26	7.5	CVE-2008-3785 MILW0RM BID
nullscripts -- web_directory_script	SQL injection vulnerability in listing_view.php in Web Directory Script 2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the name parameter.	unknown 2008-08-26	7.5	CVE-2008-3787 MILW0RM BID
OpenBSD -- OpenSSH	Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as distributed in August 2008 by servers outside Red Hat but signed with a Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: the scope of this vulnerability is restricted to users who may have obtained packages through unofficial distribution points.	unknown 2008-08-27	9.3	CVE-2008-3844 OTHER-REF REDHAT BID SECTRACK
pdesigner -- z-breaknews	SQL injection vulnerability in single.php in Z-Breaknews 2.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-08-27	7.5	CVE-2008-3848 MILW0RM BID

PicturesPro -- PicturesPro Photo Cart	Multiple SQL injection vulnerabilities in PICTURESPRO Photo Cart 3.9, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) qtitle, (2) qid, and (3) qyear parameters to (a) search.php, and the (4) email and (5) password parameters to (b) _login.php.	unknown 2008-08-26	7.5	CVE-2008-3788 MILW0RM OTHER-REF BID XF
review-script -- five_star_review_script	SQL injection vulnerability in recommend.php in Five Star Review Script allows remote attackers to execute arbitrary SQL commands via the item_id parameter.	unknown 2008-08-26	7.5	CVE-2008-3780 MILW0RM BID
SoftArtisans -- xfile	Multiple stack-based buffer overflows in the FileManager ActiveX control in SAFmgPws.dll in SoftArtisans XFile before 2.4.0 allow remote attackers to execute arbitrary code via unspecified calls to the (1) BuildPath, (2) GetDriveName, (3) DriveExists, or (4) DeleteFile method.	unknown 2008-08-27	9.3	CVE-2007-1682 OTHER-REF CERT-VN
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in the NFS Remote Procedure Calls (RPC) zones implementation in Sun Solaris 10 and OpenSolaris before snv_88 allows local administrators of non-global zones to read and modify NFS traffic for arbitrary non-global zones, possibly leading to file modifications or a denial of service.	unknown 2008-08-27	7.2	CVE-2008-3838 SUNALERT
system_consultants -- la_cooda_wiz spacetag -- lacoodast	Unspecified vulnerability in (1) System Consultants La!Cooda WIZ 1.4.0 and earlier and (2) SpaceTag LacoodaST 2.1.3 and earlier allows remote attackers to execute arbitrary PHP scripts, and delete files, read files, and possibly have unknown other impact.	unknown 2008-08-27	10.0	CVE-2008-3737 OTHER-REF OTHER-REF BID XF
Trend Micro -- OfficeScan Trend Micro -- worry_free_business_security Trend Micro -- client_server_messaging_suite	The web management console in Trend Micro OfficeScan 7.0 through 8.0, Worry-Free Business Security 5.0, and Client/Server/Messaging Suite 3.5 and 3.6 creates a random session token based only on the	unknown 2008-08-27	7.5	CVE-2008-2433 BUGTRAQ OTHER-REF OTHER-REF BID XF

	login time, which makes it easier for remote attackers to hijack sessions via brute-force attacks. NOTE: this can be leveraged for code execution through an unspecified "manipulation of the configuration."			
WordPress -- WordPress	The (1) get_edit_post_link and (2) get_edit_comment_link functions in wp-includes/link-template.php in WordPress before 2.6.1 do not force SSL communication in the intended situations, which might allow remote attackers to gain administrative access by sniffing the network for a cookie.	unknown 2008-08-27	7.5	CVE-2008-3747 MLIST MLIST

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
accellion -- file_transfer_fta	Cross-site scripting (XSS) vulnerability in Accellion File Transfer FTA_7_0_135 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to courier/forgot_password.html.	unknown 2008-08-27	4.3	CVE-2008-3850 OTHER-REF BID
aguestbook -- an_guestbook	Multiple cross-site scripting (XSS) vulnerabilities in AN Guestbook (ANG) before 0.7.6 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-08-27	4.3	CVE-2008-3847 OTHER-REF
aquagardensoft -- mysql-lists	Cross-site scripting (XSS) vulnerability in mysql-lists 1.2 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-08-27	4.3	CVE-2008-3846 OTHER-REF OTHER-REF BID
civic-cms -- civic-cms	Cross-site scripting (XSS) vulnerability in the calendar controller in Civic Website Manager before 1.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, probably involving (1) month, (2) day, and (3) year fields.	unknown 2008-08-27	4.3	CVE-2008-3849 OTHER-REF
craftysyntax -- crafty_syntax_live_help	Crafty Syntax Live Help (CSLH) 2.14.6 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain	unknown 2008-08-27	5.0	CVE-2008-3840 BUGTRAQ

	sensitive information.			
davlin -- thickbox_gallery	Davlin Thickbox Gallery 2 allows remote attackers to obtain the administrative username and MD5 password hash via a direct request to conf/admins.php.	unknown 2008-08-29	5.0	CVE-2008-3859 MILW0RM XF
Drupal -- Drupal	Cross-site scripting (XSS) vulnerability in the output filter in Drupal 5.x before 5.10 and 6.x before 6.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-08-27	4.3	CVE-2008-3740
Drupal -- Drupal	Unrestricted file upload vulnerability in the BlogAPI module in Drupal 5.x before 5.10 and 6.x before 6.4 allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, which is not validated.	unknown 2008-08-27	6.5	CVE-2008-3742 OTHER-REF
Drupal -- Drupal	Multiple cross-site request forgery (CSRF) vulnerabilities in forms in Drupal 6.x before 6.4 allow remote attackers to perform unspecified actions via unknown vectors, related to improper token validation for (1) cached forms and (2) forms with AHAH elements.	unknown 2008-08-27	5.8	CVE-2008-3743 OTHER-REF
Drupal -- Drupal	Multiple cross-site request forgery (CSRF) vulnerabilities in Drupal 5.x before 5.10 and 6.x before 6.4 allow remote attackers to (1) add or (2) delete user access rules as administrators via an unspecified URL.	unknown 2008-08-27	5.8	CVE-2008-3744
Drupal -- Drupal Drupal -- upload_module	The Upload module in Drupal 6.x before 6.4 allows remote authenticated users to edit nodes, delete files, and download unauthorized attachments via unspecified vectors.	unknown 2008-08-27	5.5	CVE-2008-3745
Fujitsu -- web_based_admin_view	Directory traversal vulnerability in Fujitsu Web-Based Admin View 2.1.2 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	unknown 2008-08-25	5.0	CVE-2008-3776 FULLDISC BID SECTRACK
gmod -- gbrowse	Cross-site scripting (XSS) vulnerability in GMOD GBrowse before 1.69 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-08-26	4.3	CVE-2008-3781 OTHER-REF
IBM -- DB2 Universal Database	Unspecified vulnerability in the DB2 Administration Server (DAS) in the Core DAS function component in IBM DB2 9.1 before Fixpak 5 allows local users to gain	unknown 2008-08-28	4.6	CVE-2008-3855 AIXAPAR BID XF

	privileges, aka a "FILE CREATION VULNERABILITY." NOTE: this may be the same as CVE-2007-5664.			
IBM -- DB2 Universal Database	The Base Service Utilities component in IBM DB2 9.1 before Fixpak 5 retains a cleartext password in memory after the database connection that sent the password is fully established, which might allow local users to obtain sensitive information by reading a memory dump.	unknown 2008-08-28	4.6	CVE-2008-3857 AIXAPAR BID
IBM -- DB2 Universal Database	The Downlevel DB2RA Support component in IBM DB2 9.1 before Fixpak 4a allows remote attackers to cause a denial of service (instance crash) via a crafted CONNECT data stream that simulates a V7 client connect request.	unknown 2008-08-28	4.3	CVE-2008-3858
matterdaddy -- matterdaddy_market	Multiple SQL injection vulnerabilities in index.php in Matterdaddy Market 1.1, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) category and (2) type parameters.	unknown 2008-08-26	6.8	CVE-2008-3783 MILW0RM BID
Microsoft -- .net_framework	Request Validation (aka the ValidateRequest filters) in ASP.NET in Microsoft .NET Framework without the MS07-040 update does not properly detect dangerous client input, which allows remote attackers to conduct cross-site scripting (XSS) attacks, as demonstrated by a query string containing a "	unknown 2008-08-27	4.3	CVE-2008-3842 BUGTRAQ OTHER-REF
Microsoft -- .net_framework	Request Validation (aka the ValidateRequest filters) in ASP.NET in Microsoft .NET Framework with the MS07-040 update does not properly detect dangerous client input, which allows remote attackers to conduct cross-site scripting (XSS) attacks, as demonstrated by a query string containing a "<~/" (less-than tilde slash) sequence followed by a crafted STYLE element.	unknown 2008-08-27	4.3	CVE-2008-3843 BUGTRAQ OTHER-REF
openfreeway -- Freeway	Cross-site scripting (XSS) vulnerability in admin/search_links.php in Freeway eCommerce 1.4.1.171 allows remote attackers to inject arbitrary web script or HTML via the search_link parameter.	unknown 2008-08-27	4.3	CVE-2008-3841 BUGTRAQ OTHER-REF

PicturesPro -- PicturesPro Photo Cart	Cross-site scripting (XSS) vulnerability in index.php in PICTURESPRO Photo Cart 3.9 allows remote attackers to inject arbitrary web script or HTML via the qtitle parameter (aka "Gallery or event name" field) in a search action.	unknown 2008-08-26	4.3	CVE-2008-3786 FULLDISC BID XF
review-script -- five_star_review_script	Cross-site scripting (XSS) vulnerability in search/index.php in Five Star Review Script allows remote attackers to inject arbitrary web script or HTML via the words parameter in a search action.	unknown 2008-08-26	4.3	CVE-2008-3779 MILW0RM BID
ruby-lang -- Ruby	The REXML module in Ruby 1.8.6 through 1.8.6-p287, 1.8.7 through 1.8.7-p72, and 1.9 allows context-dependent attackers to cause a denial of service (CPU consumption) via an XML document with recursively nested entities, aka an "XML entity explosion."	unknown 2008-08-27	5.0	CVE-2008-3790 MLIST MLIST MLIST OTHER-REF
spacetag -- lacoodast	Session fixation vulnerability in SpaceTag LacoodaST 2.1.3 and earlier allows remote attackers to hijack web sessions via unspecified vectors.	unknown 2008-08-27	6.8	CVE-2008-3738 OTHER-REF OTHER-REF BID
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in the NFS module in the kernel in Sun Solaris 10 and OpenSolaris snv_59 through snv_87, when configured as an NFS server without the nodevices option, allows local users to cause a denial of service (panic) via unspecified vectors.	unknown 2008-08-27	4.7	CVE-2008-3839 SUNALERT
swfdec -- swfdec	Swfdec 0.6 before 0.6.8 allows remote attackers to cause a denial of service (application crash) via a 1x1 JPEG image.	unknown 2008-08-27	5.0	CVE-2008-3796 MLIST MLIST
system_consultants -- la_cooda_wiz spacetag -- lacoodast	Multiple cross-site request forgery (CSRF) vulnerabilities in (1) System Consultants La!Cooda WIZ 1.4.0 and earlier and (2) SpaceTag LacoodaST 2.1.3 and earlier allow remote attackers to (a) change passwords or (b) change configurations as arbitrary users via unspecified vectors.	unknown 2008-08-27	6.0	CVE-2008-3736 OTHER-REF OTHER-REF BID XF
system_consultants -- la_cooda_wiz spacetag -- lacoodast	Cross-site scripting (XSS) vulnerability in (1) System Consultants La!Cooda WIZ 1.4.0 and earlier and (2) SpaceTag LacoodaST 2.1.3 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly involving upload of files	unknown 2008-08-27	4.3	CVE-2008-3739 OTHER-REF OTHER-REF OTHER-REF BID XF

	containing XSS sequences.			
VideoLAN -- VLC Media Player	Integer signedness error in the mms_ReceiveCommand function in modules/access/mms/mmstu.c in VLC Media Player 0.8.6i allows remote attackers to execute arbitrary code via a crafted mmst link with a negative size value, which bypasses a size check and triggers an integer overflow followed by a stack-based buffer overflow.	unknown 2008-08-26	6.8	CVE-2008-3794 MILW0RM MLIST MLIST OTHER-REF BID
webdav -- neon	neon 0.28.0 through 0.28.2 allows remote servers to cause a denial of service (NULL pointer dereference and crash) via vectors related to Digest authentication and Digest domain parameter support.	unknown 2008-08-27	5.0	CVE-2008-3746 MLIST MLIST MLIST MLIST OTHER-REF
XMLSoft -- Libxml2	libxml2 2.6.32 and earlier does not properly detect recursion during entity expansion in an attribute value, which allows context-dependent attackers to cause a denial of service (memory and CPU consumption) via a crafted XML document.	unknown 2008-08-27	4.3	CVE-2008-3281 MLIST OTHER-REF MANDRIVA REDHAT

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Avaya -- Communication Manager Avaya -- SIP Enablement Services	The SIP Enablement Services (SES) Server in Avaya SIP Enablement Services 5.0, and Communication Manager (CM) 5.0 on the S8300C with SES enabled, writes account names and passwords to the (1) alarm and (2) system logs during failed login attempts, which allows local users to obtain login credentials by reading these logs.	unknown 2008-08-25	2.1	CVE-2008-3777 OTHER-REF BID XF
discountedscripts -- acg_ptp	Multiple cross-site scripting (XSS) vulnerabilities in admin/index.php in ACG-PTP 1.0.6 allow remote authenticated administrators to inject arbitrary web script or HTML via the (1) Category name field under Advertisement Packages, the (2) Reason field under Credit/Debit Users, and the (3) FAQ question and (4) FAQ answer fields under Add New FAQ Entry.	unknown 2008-08-26	3.5	CVE-2008-3782 FULLDISC BID XF

Drupal -- Drupal	The private filesystem in Drupal 5.x before 5.10 and 6.x before 6.4 trusts the MIME type sent by a web browser, which allows remote authenticated users to conduct cross-site scripting (XSS) attacks by uploading files containing arbitrary web script or HTML.	unknown 2008-08-27	3.5	CVE-2008-3741
Pluck -- Pluck	Multiple directory traversal vulnerabilities in Pluck CMS 4.5.2 on Windows allow remote attackers to include and execute arbitrary local files via a ..\ (dot dot backslash) in the (1) blogpost, (2) cat, and (3) file parameters to data/inc/themes/predefined_variables.php, as reachable through index.php; and the (4) blogpost and (5) cat parameters to data/inc/blog_include_react.php, as reachable through index.php. NOTE: the issue involving vectors 1 through 3 reportedly exists because of an incomplete fix for CVE-2008-3194.	unknown 2008-08-27	0.0	CVE-2008-3851 BUGTRAQ MILW0RM OTHER-REF
Samba -- Samba	Samba 3.2.0 uses weak permissions (0666) for the (1) group_mapping.tdb and (2) group_mapping.ldb files, which allows local users to modify the membership of Unix groups.	unknown 2008-08-27	2.1	CVE-2008-3789 MLIST OTHER-REF

Back to top