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
1-Script -- 1-book	Static code injection vulnerability in guestbook.php in 1Book 1.0.1 and earlier allows remote attackers to upload arbitrary PHP code via the message parameter in an HTML webform, which is written to data.php.	unknown 2008-06-09	10.0	CVE-2008-2638 MILW0RM OTHER-REF XF
backweb -- backweb Logitech -- desktop_manager	Multiple stack-based buffer overflows in the BackWeb Lite Install Runner ActiveX control in the BackWeb Web Package ActiveX object in LiteInstActivator.dll in BackWeb before 8.1.1.87, as used in Logitech Desktop Manager (LDM) before 2.56, allow remote attackers to execute arbitrary code via unspecified vectors.	unknown 2008-06-11	9.3	CVE-2008-0956 OTHER-REF CERT BID
barad_dur -- bitkinex	Multiple directory traversal vulnerabilities in BitKinex 2.9.3 allow remote FTP and WebDAV servers to create or overwrite arbitrary files via a .. (dot dot) in (1) a response to a LIST command from the BitKinex FTP client and (2) a response to a PROPFIND command from the BitKinex WebDAV client. NOTE: this can be leveraged for code execution by writing to a Startup folder.	unknown 2008-06-09	9.3	CVE-2008-2635 OTHER-REF

BattleBlog -- BattleBlog	SQL injection vulnerability in comment.asp in Battle Blog 1.25 and earlier allows remote attackers to execute arbitrary SQL commands via the entry parameter.	unknown 2008-06-09	7.5	CVE-2008-2626 MILW0RM XF
BattleBlog -- BattleBlog	SQL injection vulnerability in article.asp in Battle Blog 1.25 Build 4 and earlier allows remote attackers to execute arbitrary SQL commands via the entry parameter, a different vector than CVE-2008-2626.	unknown 2008-06-12	7.5	CVE-2008-2685 OTHER-REF
bearriver -- i-pos_internet_pay_online_store	SQL injection vulnerability in index.asp in I-Pos Internet Pay Online Store 1.3 Beta and earlier allows remote attackers to execute arbitrary SQL commands via the item parameter.	unknown 2008-06-09	7.5	CVE-2008-2634 MILW0RM XF
black_ice -- barcode_sdk	The BIDIB.BIDIBCtrl.1 ActiveX control in BIDIB.ocx 10.9.3.0 in Black Ice Barcode SDK 5.01 allows remote attackers to force the download and storage of arbitrary files by specifying the origin URL in the first argument to the DownloadImageFileURL method, and the local filename in the second argument. NOTE: some of these details are obtained from third party information.	unknown 2008-06-12	9.3	CVE-2008-2683 MILW0RM XF
blackice -- black_ice_barcode_sdk	The BIDIB.BIDIBCtrl.1 ActiveX control in BIDIB.ocx 10.9.3.0 in Black Ice Barcode SDK 5.01 allows remote attackers to execute arbitrary code via long strings in the two arguments to the DownloadImageFileURL method, which trigger memory corruption. NOTE: some of these details are obtained from third party information.	unknown 2008-06-12	9.3	CVE-2008-2684 MILW0RM XF
brim-project -- brim	Multiple PHP remote file inclusion vulnerabilities in Brim (formerly Booby) 1.0.1 allow remote attackers to execute arbitrary PHP code via a URL in the renderer parameter to template.tpl.php in (1) barrel/, (2) barry/, (3) mylook/, (4) oerdec/, (5) penguin/, (6) sidebar/, (7) slashdot/, and (8) text-only/ in templates/. NOTE: this can also be leveraged to include and execute arbitrary local files via directory traversal sequences.	unknown 2008-06-10	7.5	CVE-2008-2645 MILW0RM BID XF
Cisco -- linksys_wrh54g_router	The HTTP service on the Cisco Linksys WRH54G with firmware 1.01.03 allows remote attackers to cause a denial of service (management interface outage) or	unknown 2008-06-09	7.8	CVE-2008-2636 BUGTRAQ XF

	possibly execute arbitrary code via a URI that begins with a "/./" sequence, contains many instances of a "front_page" sequence, and ends with a ".asp" sequence.			
dcfm_blog -- dcfm_blog	SQL injection vulnerability in comments.php in DCFM Blog 0.9.4 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-11	7.5	CVE-2008-2671 BUGTRAQ MILW0RM OTHER-REF BID
don3 -- DesktopOnNet	Multiple PHP remote file inclusion vulnerabilities in DesktopOnNet 3 Beta allow remote attackers to execute arbitrary PHP code via a URL in the app_path parameter to (1) don3_requiem.don3app/don3_requiem.php and (2) frontpage.don3app/frontpage.php.	unknown 2008-06-10	7.5	CVE-2008-2649 MILW0RM XF
Drupal -- LifeType Drupal -- pblog	SQL injection vulnerability in the LifeType (formerly pLog) module for Drupal allows remote attackers to execute arbitrary SQL commands via the albumId parameter in a ViewAlbum action to index.php.	unknown 2008-06-09	7.5	CVE-2008-2629 MILW0RM XF
erfurtwiki -- erfurtWiki	Multiple directory traversal vulnerabilities in ErfurtWiki R1.02b and earlier, when register_globals is enabled, allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the (1) ewiki_id and (2) ewiki_action parameters to fragments/css.php, and possibly the (3) id parameter to the default URI. NOTE: the default URI is site-specific but often performs an include_once of ewiki.php.	unknown 2008-06-11	7.5	CVE-2008-2672 BUGTRAQ MILW0RM OTHER-REF BID
insanelysimple2 -- isblog	Multiple SQL injection vulnerabilities in index.php in Insanely Simple Blog 0.5 allow remote attackers to execute arbitrary SQL commands via (1) the id parameter, or (2) the term parameter in a search action. NOTE: the current_subsection parameter is already covered by CVE-2007-3889.	unknown 2008-06-11	7.5	CVE-2008-2670 BUGTRAQ MILW0RM OTHER-REF BID
Joomla -- com_simpleshop Joomla -- Joomla	SQL injection vulnerability in the Simple Shop Galore (com_simpleshop) component 3.4 and earlier for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter in a browse action to index.php.	unknown 2008-06-06	7.5	CVE-2008-2568 MILW0RM
Joomla -- com_idoblog	SQL injection vulnerability in the IDoBlog (com_idoblog) component b24 and earlier and 1.0, a component for Joomla!, allows	unknown 2008-06-09	7.5	CVE-2008-2627 MILW0RM XF

	remote attackers to execute arbitrary SQL commands via the userid parameter in a userblog action to index.php.			
Joomla -- com_equotes Joomla -- Joomla	SQL injection vulnerability in the eQuotes (com_equotes) component 0.9.4 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	unknown 2008-06-09	7.5	CVE-2008-2628 MILW0RM XF
Joomla -- com_jb2	SQL injection vulnerability in the JooBlog (com_jb2) component 0.1.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the CategoryID parameter in a category action to index.php.	unknown 2008-06-09	7.5	CVE-2008-2630 MILW0RM
Joomla -- com_acctexp Joomla -- Joomla	SQL injection vulnerability in the acctexp (com_acctexp) component 0.12.x and earlier for Joomla! allows remote attackers to execute arbitrary SQL commands via the usage parameter in a subscribe action to index.php.	unknown 2008-06-09	7.5	CVE-2008-2632 MILW0RM XF
Joomla -- com_joomradio Joomla -- Joomla	Multiple SQL injection vulnerabilities in the EXP JoomRadio (com_joomradio) component 1.0 for Joomla! allow remote attackers to execute arbitrary SQL commands via the id parameter in a (1) show_radio or (2) show_video action to index.php.	unknown 2008-06-09	7.5	CVE-2008-2633 MILW0RM XF
Joomla -- com_biblestudy	SQL injection vulnerability in the Bible Study (com_biblestudy) component before 6.0.7c for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a mediaplayer action to index.php.	unknown 2008-06-10	7.5	CVE-2008-2643 MILW0RM OTHER-REF XF
Joomla -- com_joobb	SQL injection vulnerability in the Joomla! Bulletin Board (aka Joo!BB or com_joobb) component 0.5.9 for Joomla! allows remote attackers to execute arbitrary SQL commands via the forum parameter in a forum action to index.php.	unknown 2008-06-10	7.5	CVE-2008-2651 MILW0RM XF
Joomla -- com_news_portal Joomla -- Joomla	SQL injection vulnerability in the iJoomla News Portal (com_news_portal) component 1.0 and earlier for Joomla! allows remote attackers to execute arbitrary SQL commands via the Itemid parameter to index.php.	unknown 2008-06-12	7.5	CVE-2008-2676 MILW0RM XF
KMRG-ITB -- otomigenx	SQL injection vulnerability in login.php in OtomiGenX 2.2 allows remote attackers to execute arbitrary SQL commands via the userAccount parameter (aka the User	unknown 2008-06-10	7.5	CVE-2008-2642 BUGTRAQ XF

	Name field) to index.php. NOTE: some of these details are obtained from third party information.			
Linux -- Kernel Debian -- Debian Linux	The asn1 implementation in (a) the Linux kernel 2.4 before 2.4.36.6 and 2.6 before 2.6.25.5, as used in the cifs and ip_nat_snmp_basic modules; and (b) the gxsnmp package; does not properly validate length values during decoding of ASN.1 BER data, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via (1) a length greater than the working buffer, which can lead to an unspecified overflow; (2) an oid length of zero, which can lead to an off-by-one error; or (3) an indefinite length for a primitive encoding.	unknown 2008-06-09	10.0	CVE-2008-1673 OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF XF SECTRACK SECUNIA
Linux -- Kernel	The Datagram Congestion Control Protocol (DCCP) subsystem in the Linux kernel 2.6.18, and probably other versions, does not properly check feature lengths, which might allow remote attackers to execute arbitrary code, related to an unspecified "overflow."	unknown 2008-06-09	7.5	CVE-2008-2358 BID SECTRACK SECUNIA
mebiblio -- mebiblio	SQL injection vulnerability in admin/journal_change_mask.inc.php in meBiblio 0.4.7 allows remote attackers to execute arbitrary SQL commands via the JID parameter.	unknown 2008-06-10	7.5	CVE-2008-2647 MILW0RM BID XF
Microsoft -- DirectX	Microsoft DirectX 8.1 through 9.0c, and DirectX on Microsoft XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008, does not properly perform MJPEG error checking, which allows remote attackers to execute arbitrary code via a crafted MJPEG stream in a (1) AVI or (2) ASF file, aka the "MJPEG Decoder Vulnerability."	unknown 2008-06-11	9.3	CVE-2008-0011 CERT
Microsoft -- windows Microsoft -- windows-nt	Microsoft Windows XP SP2 and SP3, and Server 2003 SP1 and SP2, does not properly validate the option length field in Pragmatic General Multicast (PGM) packets, which allows remote attackers to cause a denial of service (infinite loop and system hang) via a crafted PGM packet, aka the "PGM Invalid Length Vulnerability."	unknown 2008-06-11	7.1	CVE-2008-1440 CERT SECTRACK
Microsoft -- Internet Explorer	Heap-based buffer overflow in the substringData method in Microsoft Internet Explorer 6 and 7 allows remote	unknown 2008-06-11	9.3	CVE-2008-1442 BUGTRAQ CERT

	attackers to execute arbitrary code, related to an unspecified manipulation of a DOM object before a call to this method, aka the "HTML Objects Memory Corruption Vulnerability."			
Microsoft -- DirectX	Stack-based buffer overflow in Microsoft DirectX 7.0 and 8.1 on Windows 2000 SP4 allows remote attackers to execute arbitrary code via a Synchronized Accessible Media Interchange (SAMI) file with crafted parameters for a Class Name variable, aka the "SAMI Format Parsing Vulnerability."	unknown 2008-06-11	9.3	CVE-2008-1444 BUGTRAQ CERT SECTRACK
Microsoft -- windows-nt	Active Directory on Microsoft Windows 2000 Server SP4, XP Professional SP2 and SP3, Server 2003 SP1 and SP2, and Server 2008 allows remote authenticated users to cause a denial of service (system hang or reboot) via a crafted LDAP request.	unknown 2008-06-11	7.1	CVE-2008-1445 CERT SECTRACK
Microsoft -- windows-nt	The WINS service on Microsoft Windows 2000 SP4, and Server 2003 SP1 and SP2, does not properly validate data structures in WINS network packets, which allows local users to gain privileges via a crafted packet, aka "Memory Overwrite Vulnerability."	unknown 2008-06-11	7.2	CVE-2008-1451 CERT
Microsoft -- windows-nt	The Bluetooth stack in Microsoft Windows XP SP2 and SP3, and Vista Gold and SP1, allows physically proximate attackers to execute arbitrary code via a large series of Service Discovery Protocol (SDP) packets.	unknown 2008-06-11	8.3	CVE-2008-1453 CERT
OpenOffice -- OpenOffice.org	Integer overflow in the rtl_allocateMemory function in sal/rtl/source/alloc_global.c in OpenOffice.org (OOo) 2.0 through 2.4 allows remote attackers to execute arbitrary code via a crafted file that triggers a heap-based buffer overflow.	unknown 2008-06-10	9.3	CVE-2008-2152 IDEFENSE OTHER-REF BID
opensuse -- opensuse	Multiple off-by-one errors in opensuse-updater in openSUSE 10.2 have unspecified impact and attack vectors. NOTE: the vendor states that these "can be considered no security problem."	unknown 2008-06-06	10.0	CVE-2008-2388 SUSE
Powie -- pnews	SQL injection vulnerability in index.php in Powie pNews 2.08 and 2.10, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the shownews parameter.	unknown 2008-06-12	7.5	CVE-2008-2673 MILW0RM

realm_project -- realm_cms	SQL injection vulnerability in the KeyWordsList function in _includes/inc_routines.asp in Realm CMS 2.3 and earlier allows remote attackers to execute arbitrary SQL commands via the kwrd parameter in a kwl action to the default URI.	unknown 2008-06-12	7.5	CVE-2008-2679 MILW0RM OTHER-REF
realm_project -- realm_cms	_RealmAdmin/login.asp in Realm CMS 2.3 and earlier allows remote attackers to bypass authentication and access admin pages via certain modified cookies, probably including (1) cUserRole, (2) cUserName, and (3) cUserID.	unknown 2008-06-12	7.5	CVE-2008-2682 MILW0RM OTHER-REF
smeweb -- smeweb	Multiple SQL injection vulnerabilities in catalog.php in SMEWeb 1.4b and 1.4f allow remote attackers to execute arbitrary SQL commands via the (1) idp and (2) category parameters.	unknown 2008-06-10	7.5	CVE-2008-2652 MILW0RM
telephone -- Telephone Directory 2008	Multiple SQL injection vulnerabilities in Telephone Directory 2008, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) code parameter in a confirm_data action to edit1.php and the (2) id parameter to view_more.php.	unknown 2008-06-12	7.5	CVE-2008-2678 MILW0RM
y-blog -- yblog	Multiple SQL injection vulnerabilities in yBlog 0.2.2.2 allow remote attackers to execute arbitrary SQL commands via (1) the q parameter to search.php, or the n parameter to (2) user.php or (3) uss.php.	unknown 2008-06-11	7.5	CVE-2008-2669 BUGTRAQ MILW0RM OTHER-REF BID XF

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
SNMP v3	SNMPv3 HMAC verification in (1) Net-SNMP 5.2.x before 5.2.4.1, 5.3.x before 5.3.2.1, and 5.4.x before 5.4.1.1; (2) UCD-SNMP; (3) eCos; (4) Juniper Session and Resource Control (SRC) C-series 1.0.0 through 2.0.0; (5) NetApp (aka Network Appliance) Data ONTAP 7.3RC1 and 7.3RC2; (6) SNMP Research before 16.2; and (7) multiple Cisco IOS, CatOS, ACE, and Nexus products; relies on the client to specify the HMAC length, which makes it easier for remote attackers to bypass SNMP authentication via a length value of 1, which only checks the first byte.	unknown 2008-06-10	6.8	CVE-2008-0960 BUGTRAQ MLIST OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF OTHER-REF REDHAT CERT-VN BID

				CERT
Alt-N -- MDaemon	The WordClient interface in Alt-N Technologies MDaemon 9.6.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted HTTP POST request. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-09	5.0	CVE-2008-2631 XF
Apple -- Quicktime	Heap-based buffer overflow in Apple QuickTime before 7.5 on Windows allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted packed scanlines in PixData structures in a PICT image.	unknown 2008-06-10	6.8	CVE-2008-1581
Apple -- Quicktime	Unspecified vulnerability in Apple QuickTime before 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted AAC-encoded file that triggers memory corruption.	unknown 2008-06-10	6.8	CVE-2008-1582
Apple -- Quicktime	Heap-based buffer overflow in Apple QuickTime before 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PICT image, a different vulnerability than CVE-2008-1581.	unknown 2008-06-10	6.8	CVE-2008-1583
Apple -- Quicktime	Stack-based buffer overflow in Apple QuickTime before 7.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted Indeo video codec content in a movie file.	unknown 2008-06-10	6.8	CVE-2008-1584
Apple -- Quicktime	Apple QuickTime before 7.5 allows remote attackers to execute arbitrary programs via crafted file: URLs.	unknown 2008-06-10	6.8	CVE-2008-1585
CMSimple -- CMSimple	Directory traversal vulnerability in cmsimple/cms.php in CMSimple 3.1, when register_globals is enabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the sl parameter to index.php. NOTE: this can be leveraged for remote file execution by including adm.php and then invoking the upload action. NOTE: on 20080601, the vendor patched 3.1 without changing the version number.	unknown 2008-06-10	6.8	CVE-2008-2650 MILW0RM OTHER-REF BID
F5 -- firepass_ssl_vpn	Multiple cross-site scripting (XSS) vulnerabilities in F5 FirePass SSL VPN 6.0.2 hotfix 3, and possibly earlier versions, allow remote attackers to inject arbitrary web script or HTML via quotes in (1) the css_exceptions parameter in webyfiers.php and (2) the sql_matchscope parameter in index.php.	unknown 2008-06-09	4.3	CVE-2008-2637 BUGTRAQ BID SECTRACK

Fujitsu -- Interstage Application Server Standard_J Fujitsu -- Interstage Studio Enterprise Fujitsu -- Interstage Apworks Modelers_J Fujitsu -- Interstage Application Server Plus Fujitsu -- interstage application server plus developer Fujitsu -- interstage business application server enterprise Fujitsu -- Interstage Studio Standard_J Fujitsu -- Interstage Application Server Enterprise	Unspecified vulnerability in the Interstage Management Console, as used in Fujitsu Interstage Application Server 6.0 through 9.0.0A, Apworks Modelers-J 6.0 through 7.0, and Studio 8.0.1 and 9.0.0, allows remote attackers to read or delete arbitrary files via unspecified vectors.	unknown 2008-06-12	6.4	CVE-2008-2674 OTHER-REF
mebiblio -- mebiblio	Multiple cross-site scripting (XSS) vulnerabilities in meBiblio 0.4.7 allow remote attackers to inject arbitrary web script or HTML via the (1) sql parameter to dbadd.inc.php, (2) InsertJournal parameter to add_journal_mask.inc.php, (3) InsertBibliography parameter to insert_mask.inc.php, and (4) LabelYear parameter to search_mask.inc.php.	unknown 2008-06-10	4.3	CVE-2008-2646 MILW0RM BID XF
mebiblio -- mebiblio	Unrestricted file upload vulnerability in upload/uploader.html in meBiblio 0.4.7 allows remote attackers to execute arbitrary code by uploading a .php file, then accessing it via a direct request to the files/ directory.	unknown 2008-06-10	6.8	CVE-2008-2648 MILW0RM BID XF
Microsoft -- windows-nt	Microsoft Windows XP SP2 and SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote attackers to cause a denial of service (system hang) via a series of Pragmatic General Multicast (PGM) packets with invalid fragment options, aka the "PGM Malformed Fragment Vulnerability."	unknown 2008-06-11	5.4	CVE-2008-1441 CERT BID SECTRACK
realm_project -- realm_cms	Multiple cross-site scripting (XSS) vulnerabilities in _db/compact.asp in Realm CMS 2.3 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) CmpctedDB and (2) Boyut parameters.	unknown 2008-06-12	4.3	CVE-2008-2680 MILW0RM OTHER-REF
realm_project -- realm_cms	Realm CMS 2.3 and earlier allows remote attackers to obtain sensitive information via a direct request to _db/compact.asp, which reveals the database path in an error message.	unknown 2008-06-12	5.0	CVE-2008-2681 MILW0RM OTHER-REF

reportbug-ng -- reportbug-ng reportbug-ng -- reportbug	Untrusted search path vulnerability in (1) reportbug 3.8 and 3.31, and (2) reportbug-ng before 0.2008.06.04, allows local users to execute arbitrary code via a malicious module file in the current working directory.	unknown 2008-06-10	4.6	CVE-2008-2230 OTHER-REF OTHER-REF
smeweb -- smeweb	Multiple cross-site scripting (XSS) vulnerabilities in SMEWeb 1.4b and 1.4f allow remote attackers to inject arbitrary web script or HTML via the (1) data parameter to catalog.php, the (2) keyword parameter to search.php, the (3) page parameter to bb.php, and the (4) new_s parameter to order.php.	unknown 2008-06-10	4.3	CVE-2008-2644 MILW0RM
SoftComplex -- PHP Image Gallery	Cross-site scripting (XSS) vulnerability in index.php in PHP Image Gallery allows remote attackers to inject arbitrary web script or HTML via the action parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-12	4.3	CVE-2008-2675
telephone -- Telephone Directory 2008	Cross-site scripting (XSS) vulnerability in edit1.php in Telephone Directory 2008 allows remote attackers to inject arbitrary web script or HTML via the action parameter.	unknown 2008-06-12	4.3	CVE-2008-2677 MILW0RM
y-blog -- yblog	Multiple cross-site scripting (XSS) vulnerabilities in yBlog 0.2.2.2 allow remote attackers to inject arbitrary web script or HTML via (1) the q parameter to search.php, or the n parameter to (2) user.php or (3) uss.php.	unknown 2008-06-11	4.3	CVE-2008-2668 BUGTRAQ MILW0RM OTHER-REF BID XF

Back to top

There were no low vulnerabilities recorded this week.