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<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| 8e6 -- R3000 Internet Filter | 8e6 R3000 Internet Filter 2.0.12.10 allows remote attackers to bypass intended restrictions via an extra HTTP Host header with additional leading text placed before the real Host header. | unknown<br>2008-08-06 | 7.8 | CVE-2008-3494<br>BUGTRAQ<br>BID |
| Apple -- iTunes | Apple iTunes before 6.0.5.20 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning. | unknown<br>2008-08-01 | 7.5 | CVE-2008-3434<br>FULLDISC<br>OTHER-REF |
| Aspindir -- pcshey_portal | SQL injection vulnerability in kategori.asp in Pcshey Portal allows remote attackers to execute arbitrary SQL commands via the kid parameter. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3495<br>OTHER-REF<br>BID<br>XF |

| | | | | |
|---|---|---|---|---|
| bestpractical -- request_tracker | Unspecified vulnerability in Best Practical Solutions RT 3.0.0 through 3.6.6 allows remote authenticated users to cause a denial of service (CPU or memory consumption) via unspecified vectors related to the Devel::StackTrace module for Perl. | unknown<br>2008-08-06 | 9.0 | CVE-2008-3502<br>MLIST<br>BID<br>XF |
| Citrix -- xp<br>Citrix -- MetaFrame Presentation Server | Untrusted search path vulnerability in Citrix MetaFrame Presentation Server allows local users to gain privileges via a malicious icabar.exe placed in the search path. | unknown<br>2008-08-06 | 7.2 | CVE-2008-3485<br>BUGTRAQ<br>BID |
| coppermine-gallery -- coppermine_photo_gallery | themes/sample/theme.php in Coppermine Photo Gallery (CPG) 1.4.18 and earlier allows remote attackers to obtain sensitive information via a direct request, which reveals the installation path in an error message. | unknown<br>2008-08-05 | 7.5 | CVE-2008-3481<br>MILW0RM |
| coppermine-gallery -- coppermine_photo_gallery | Directory traversal vulnerability in the user_get_profile function in include/functions.inc.php in Coppermine Photo Gallery (CPG) 1.4.18 and earlier, when the charset is utf-8, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang part of serialized data in an _data cookie. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3486<br>MILW0RM<br>BID |
| ektron -- cms4000.net | Unspecified vulnerability in "a page in the workarea folder" in Ektron CMS400.NET 7.00 through 7.04 and 7.50 through 7.52 has unknown impact and attack vectors. | unknown<br>2008-08-06 | 10.0 | CVE-2008-3499 |
| estoreaff -- estoreaff | SQL injection vulnerability in eStoreAff 0.1 allows remote attackers to execute arbitrary SQL commands via the cid parameter in a showcat action to index.php. | unknown<br>2008-08-05 | 7.5 | CVE-2008-3484<br>MILW0RM<br>BID |
| GIT -- GIT | Stack-based buffer overflow in the (1) diff_addremove and (2) diff_change functions in GIT before 1.5.6.4 might allow local users to execute arbitrary code via a PATH whose length is larger than the system's PATH_MAX when running GIT utilities such as git-diff or git-grep. | unknown<br>2008-08-07 | 7.5 | CVE-2008-3546<br>MLIST<br>OTHER-REF<br>BID<br>SECTRACK |

| | | | | |
|---|---|---|---|---|
| impresscms -- impresscms | Multiple unspecified vulnerabilities in ImpressCMS 1.0 have unknown impact and attack vectors, related to modules/admin.php and "a few files." | unknown<br>2008-08-04 | 10.0 | CVE-2008-3453<br>OTHER-REF<br>SECUNIA |
| Ingres -- Ingres | Untrusted search path vulnerability in ingvalidpw in Ingres 2.6, Ingres 2006 release 1 (aka 9.0.4), and Ingres 2006 release 2 (aka 9.1.0) on Linux and HP-UX allows local users to gain privileges via a crafted shared library, related to a "pointer overwrite vulnerability." | unknown<br>2008-08-05 | 7.2 | CVE-2008-3357<br>IDEFENSE<br>OTHER-REF<br>BID<br>SECTRACK |
| JnSHosts -- php_hosting_directory | JnSHosts PHP Hosting Directory 2.0 allows remote attackers to bypass authentication and gain administrative access by setting the "adm" cookie value to 1. | unknown<br>2008-08-04 | 7.5 | CVE-2008-3454<br>MILW0RM<br>BID |
| JnSHosts -- php_hosting_directory | PHP remote file inclusion vulnerability in include/admin.php in JnSHosts PHP Hosting Directory 2.0 allows remote attackers to execute arbitrary PHP code via a URL in the rd parameter. | unknown<br>2008-08-04 | 10.0 | CVE-2008-3455<br>MILW0RM<br>BID |
| Joomla -- com_netinvoice | SQL injection vulnerability in the nBill (com_netinvoice) component 1.2.0 SP1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the cid parameter in an orders action to index.php. NOTE: some of these details are obtained from third party information. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3498<br>MILW0RM |
| Linux -- Kernel | Buffer overflow in format descriptor parsing in the uvc_parse_format function in drivers/media/video/uvc/uvc_driver.c in uvcvideo in the video4linux (V4L) implementation in the Linux kernel before 2.6.26.1 has unknown impact and attack vectors. | unknown<br>2008-08-06 | 10.0 | CVE-2008-3496<br>MLIST<br>OTHER-REF<br>BID<br>XF |
| LoveCMS -- LoveCMS | LoveCMS 1.6.2 does not require administrative authentication for (1) addblock.php, (2) blocks.php, and (3) themes.php in system/admin/, which allows remote attackers to change the configuration or execute | unknown<br>2008-08-07 | 7.5 | CVE-2008-3509 |

| | | | | |
|---|---|---|---|---|
| | arbitrary PHP code, related to "inserted page blocks." NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | | | |
| mpfm -- mask_php_file_manager | Unspecified vulnerability in mask PHP File Manager (mPFM) before 2.3 has unknown impact and remote attack vectors related to "manipulation of cookies." | unknown<br>2008-08-06 | 7.5 | CVE-2008-3504<br>OTHER-REF<br>BID<br>XF |
| Notepad++ -- Notepad++ | The GUP generic update process in Notepad++ before 4.8.1 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning. | unknown<br>2008-08-01 | 7.5 | CVE-2008-3436<br>FULLDISC<br>OTHER-REF |
| Novell -- iManager | Unspecified vulnerability in Novell iManager before 2.7 SP1 (2.7.1) allows remote attackers to delete Plug-in Studio created Property Book Pages via unknown vectors. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3488 |
| Nullsoft -- Winamp | Nullsoft Winamp before 5.24 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning. | unknown<br>2008-08-01 | 7.5 | CVE-2008-3441<br>FULLDISC<br>OTHER-REF<br>SECTRACK |
| OpenVPN -- OpenVPN | Unspecified vulnerability in OpenVPN 2.1-beta14 through 2.1-rc8, when running on non-Windows systems, allows remote servers to execute arbitrary commands via crafted (1) "lladdr" and (2) "iproute" configuration directives, probably related to shell metacharacters. | unknown<br>2008-08-04 | 10.0 | CVE-2008-3459<br>OTHER-REF |
| php_nuke -- Kleinanzeigen module | SQL injection vulnerability in the Kleinanzeigen module for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the lid parameter in a visit action to modules.php. | unknown<br>2008-08-07 | 7.5 | CVE-2008-3512<br>BUGTRAQ |

| | | | | |
|---|---|---|---|---|
| php_nuke -- basis_consultant_book_catalog | SQL injection vulnerability in the Book Catalog module 1.0 for PHP-Nuke allows remote attackers to execute arbitrary SQL commands via the catid parameter in a category action to modules.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | unknown<br>2008-08-07 | 7.5 | CVE-2008-3513<br>OTHER-REF<br>BID |
| phpauctions -- phpauction_gpl_enhanced | SQL injection vulnerability in profile.php in PHPAuction GPL Enhanced 2.51 allows remote attackers to execute arbitrary SQL commands via the id parameter. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3487<br>MILW0RM<br>BID |
| phpMyRealty -- phpMyRealty | SQL injection vulnerability in index.php in phpMyRealty (PMR) 2.0.0 allows remote attackers to execute arbitrary SQL commands via the location parameter. | unknown<br>2008-08-04 | 7.5 | CVE-2008-3445<br>MILW0RM<br>BID |
| PHPX -- PHPX | SQL injection vulnerability in checkCookie function in includes/functions.inc.php in PHPX 3.5.16 allows remote attackers to execute arbitrary SQL commands via a PXL cookie. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3489<br>MILW0RM<br>BID |
| polypager -- polypager | SQL injection vulnerability in PolyPager 1.0 rc2 and earlier allows remote attackers to execute arbitrary SQL commands via the nr parameter to the default URI. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3506<br>MILW0RM |
| 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) | unknown<br>2008-08-01 | 7.5 | CVE-2008-3143<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>GENTOO |

| | | | | |
|---|---|---|---|---|
| | compile.c in Python/, as addressed by "checks for integer overflows, contributed by Google." | | | |
| scripts24 -- itgp<br>scripts24 -- ipost | SQL injection vulnerability in go.php in Scripts24 iPost 1.0.1 and iTGP 1.0.4 allows remote attackers to execute arbitrary SQL commands via the id parameter in a report action. | unknown<br>2008-08-06 | 7.5 | CVE-2008-3491<br>MILW0RM<br>MILW0RM<br>BID<br>BID |
| speedbit -- speedbit_video_accelerator | SpeedBit Video Acceleration before 2.2.1.8 does not properly verify the authenticity of updates, which allows man-in-the-middle attackers to execute arbitrary code via a Trojan horse update, as demonstrated by evilgrade and DNS cache poisoning. | unknown<br>2008-08-01 | 7.5 | CVE-2008-3439<br>FULLDISC<br>OTHER-REF |
| Sun -- xvm_virtualbox | The VBoxDrvNtDeviceControl function in VBoxDrv.sys in Sun xVM VirtualBox before 1.6.4 uses the METHOD_NEITHER communication method for IOCTLs and does not properly validate a buffer associated with the Irp object, which allows local users to gain privileges by opening the \\.\VBoxDrv device and calling DeviceIoControl to send a crafted kernel address. | unknown<br>2008-08-05 | 7.2 | CVE-2008-3431<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>SUNALERT<br>BID<br>SECTRACK |
| wogan_may -- litenews | SQL injection vulnerability in index.php in LiteNews 0.1 (aka 01), and possibly 1.2 and earlier, allows remote attackers to execute arbitrary SQL commands via the id parameter in a view action. | unknown<br>2008-08-07 | 7.5 | CVE-2008-3507<br>MILW0RM |

Back to top

## Medium Vulnerabilities

| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| americasarmy -- America's Army | America's Army (aka AA or Army Game Project) 2.8.3.1 and earlier allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted UDP packet, probably involving a VoiceIndex value that is outside of the range specified by | unknown<br>2008-08-06 | 5.0 | CVE-2008-3492<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>XF |

| | | | | |
|---|---|---|---|---|
| | VOICE_MAX_CHATTERS. | | | |
| Apache Software Foundation -- Tomcat | Cross-site scripting (XSS) vulnerability in Apache Tomcat 4.1.0 through 4.1.37, 5.5.0 through 5.5.26, and 6.0.0 through 6.0.16 allows remote attackers to inject arbitrary web script or HTML via a crafted string that is used in the message argument to the HttpServletResponse.sendError method. | unknown<br>2008-08-03 | 4.3 | CVE-2008-1232<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF |
| Apache Software Foundation -- Apache | Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via wildcards in a pathname in an FTP URI. | unknown<br>2008-08-06 | 4.3 | CVE-2008-2939<br>OTHER-REF<br>OTHER-REF<br>BID |
| Apple -- Mac OS X Server<br>Apple -- Mac OS X | The Repair Permissions tool in Disk Utility in Apple Mac OS X 10.4.11 adds the setuid bit to the emacs executable file, which allows local users to gain privileges by executing commands within emacs. | unknown<br>2008-08-03 | 4.6 | CVE-2008-2324<br>APPLE<br>BID<br>BID |
| Crafty Syntax Live Help -- Crafty Syntax Live Help | Cross-site scripting (XSS) vulnerability in livehelp_js.php in Crafty Syntax Live Help (CSLH) 2.14.6 allows remote attackers to inject arbitrary web script or HTML via the department parameter. | unknown<br>2008-08-07 | 4.3 | CVE-2008-3510<br>OTHER-REF<br>BID |
| Drupal -- suggested_terms_module | Cross-site scripting (XSS) vulnerability in the Suggested Terms module 5.x before 5.x-1.2 for Drupal allows remote authenticated users to inject arbitrary web script or HTML via crafted Taxonomy terms. | unknown<br>2008-08-06 | 4.3 | CVE-2008-3500<br>OTHER-REF |
| e-topbiz -- online_dating | SQL injection vulnerability in members/mail.php in E-topbiz Online Dating 3 1.0 allows remote authenticated users to execute arbitrary SQL commands via the mail_id parameter in a veiw action. | unknown<br>2008-08-06 | 6.5 | CVE-2008-3490<br>MILW0RM<br>BID |
| eNdonesia -- calendar_module<br>eNdonesia -- eNdonesia | SQL injection vulnerability in the Calendar module in eNdonesia 8.4 allows remote attackers to execute arbitrary SQL commands via the loc_id parameter in a list_events action to mod.php. | unknown<br>2008-08-04 | 6.8 | CVE-2008-3452<br>MILW0RM<br>BID |

| | | | | |
|---|---|---|---|---|
| Ingres -- Ingres | verifydb in Ingres 2.6, Ingres 2006 release 1 (aka 9.0.4), and Ingres 2006 release 2 (aka 9.1.0) on Linux and other Unix platforms sets the ownership or permissions of an iivdb.log file without verifying that it is the application's own log file, which allows local users to overwrite arbitrary files by creating a symlink with an iivdb.log filename. | unknown<br>2008-08-05 | 4.6 | CVE-2008-3356<br>IDEFENSE<br>OTHER-REF<br>BID<br>SECTRACK |
| Ingres -- Ingres | Stack-based buffer overflow in the libbecompat library in Ingres 2.6, Ingres 2006 release 1 (aka 9.0.4), and Ingres 2006 release 2 (aka 9.1.0) on Linux and HP-UX allows local users to gain privileges by setting a long value of an environment variable before running (1) verifydb, (2) iimerge, or (3) csreport. | unknown<br>2008-08-05 | 4.6 | CVE-2008-3389<br>IDEFENSE<br>OTHER-REF<br>BID<br>SECTRACK |
| MyPHP CMS -- MyPHP CMS | SQL injection vulnerability in pages.php in MyPHP CMS 0.3.1 allows remote attackers to execute arbitrary SQL commands via the pid parameter. | unknown<br>2008-08-06 | 6.8 | CVE-2008-3497<br>MILW0RM<br>BID<br>XF |
| Novell -- Groupwise | Cross-site scripting (XSS) vulnerability in the WebAccess simple interface in Novell Groupwise 7.0.x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2008-08-06 | 4.3 | CVE-2008-3501<br>BID<br>XF |
| Panasonic -- BB_HCM511<br>Panasonic -- BL_C131<br>Panasonic -- BB_HCM531<br>Panasonic -- BB_HCM527<br>Panasonic -- BB_HCM580<br>Panasonic -- BB_HCM515<br>Panasonic -- BL_C111<br>Panasonic -- BB_HCM581 | Cross-site scripting (XSS) vulnerability in the error page feature in Panasonic Network Camera BL-C111, BL-C131, BB-HCM511, BB-HCM531, BB-HCM580, BB-HCM581, BB-HCM527, and BB-HCM515 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2008-08-05 | 4.3 | CVE-2008-3482<br>OTHER-REF<br>OTHER-REF |
| phpMyAdmin -- phpMyAdmin | phpMyAdmin before 2.11.8 does not sufficiently prevent its pages from using frames that point to pages in other domains, which makes it easier for remote attackers to conduct spoofing or phishing activities via a cross-site framing attack. | unknown<br>2008-08-04 | 6.4 | CVE-2008-3456<br>OTHER-REF<br>OTHER-REF |

| | | | | |
|---|---|---|---|---|
| PhpWebGallery -- PhpWebGallery | PhpWebGallery 1.7.0 and 1.7.1 allows remote authenticated users with advisor privileges to obtain the real e-mail addresses of other users by editing the user's profile. | unknown<br>2008-08-04 | 4.0 | CVE-2008-3451<br>MLIST<br>OTHER-REF<br>OTHER-REF<br>XF |
| polypager -- polypager | Cross-site scripting (XSS) vulnerability in PolyPager 1.0 rc2 and earlier allows remote attackers to inject arbitrary web script or HTML via the nr parameter to the default URI. | unknown<br>2008-08-06 | 4.3 | CVE-2008-3505<br>MILW0RM |
| RealVNC -- realvnc_windows_client | vncviewer.exe in RealVNC Windows Client 4.1.2.0 allows remote VNC servers to cause a denial of service (application crash) via a crafted frame buffer update packet. | unknown<br>2008-08-06 | 5.0 | CVE-2008-3493<br>MILW0RM<br>BID |
| screwturn -- screwturn_wiki | Cross-site scripting (XSS) vulnerability in ScrewTurn Wiki 2.0.29 and 2.0.30 allows remote attackers to inject arbitrary web script or HTML via error messages in the "/admin.aspx - System Log" page. | unknown<br>2008-08-05 | 4.3 | CVE-2008-3483<br>OTHER-REF<br>OTHER-REF<br>BID |
| SoftBiz -- Image Gallery | Multiple cross-site scripting (XSS) vulnerabilities in Softbiz Image Gallery (Photo Gallery) allow remote attackers to inject arbitrary web script or HTML via the (1) latest parameter to (a) index.php, (b) images.php, (c) suggest_image.php, and (d) image_desc.php; and the (2) msg parameter to index.php, images.php, and suggest_image.php, and (e) index.php, (f) adminhome.php, (g) config.php, (h) changepassword.php, (i) cleanup.php, (j) browsecats.php, and (k) images.php in admin/. NOTE: the image_desc.php/msg vector is covered by CVE-2006-1660. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. | unknown<br>2008-08-07 | 4.3 | CVE-2008-3511<br>OTHER-REF<br>BID |
| Sun -- Netra T5220 Server | Unspecified vulnerability in the Sun Netra T5220 Server with firmware 7.1.3 allows local users to cause a denial of service (panic) via unknown vectors. | unknown<br>2008-08-07 | 4.9 | CVE-2008-3548 |
| Sun -- opensolaris<br>Sun -- Solaris | Unspecified vulnerability in the pthread_mutex_reltimedlock_np API in Sun Solaris 10 and OpenSolaris before snv_90 allows local users to cause a denial of service (system hang or panic) | unknown<br>2008-08-07 | 4.7 | CVE-2008-3549 |

| | | | | |
|---|---|---|---|---|
| | via unknown vectors. | | | |
| vtiger -- vtiger_crm | Vtiger CRM before 5.0.4 stores sensitive information under the web root with insufficient access control, which allows remote attackers to read mail merge templates via a direct request to the wordtemplatedownload directory. | unknown<br>2008-08-04 | 5.0 | CVE-2008-3458<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>OSVDB |
| WebGUI -- plain_black_webgui | RSSFromParent in Plain Black WebGUI before 7.5.13 does not restrict view access to Collaboration System (CS) RSS feeds, which allows remote attackers to obtain sensitive information (CS data). | unknown<br>2008-08-06 | 5.0 | CVE-2008-3503<br>OTHER-REF<br>OTHER-REF<br>BID<br>XF |
| wogan_may -- litenews | LiteNews 0.1 (aka 01), and possibly 1.2 and earlier, allows remote attackers to bypass authentication and gain administrative access by setting the admin cookie. | unknown<br>2008-08-07 | 5.0 | CVE-2008-3508<br>MILW0RM<br>BID |

Back to top

## Low Vulnerabilities

| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| phpMyAdmin -- phpMyAdmin | Cross-site scripting (XSS) vulnerability in setup.php in phpMyAdmin before 2.11.8 allows user-assisted remote attackers to inject arbitrary web script or HTML via crafted setup arguments. NOTE: this issue can only be exploited in limited scenarios in which the attacker must be able to modify config/config.inc.php. | unknown<br>2008-08-04 | 2.6 | CVE-2008-3457<br>OTHER-REF<br>OTHER-REF |

Back to top