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
Achievo -- Achievo	Unrestricted file upload in the mcpuk file editor (atk/attributes/fck/editor/filemanager/browser/mcpuk/connectors/php/config.php) in Achievo 1.2.0 through 1.3.2 allows remote attackers to execute arbitrary code by uploading a file with .php followed by a safe extension, then accessing it via a direct request to the file in the Achievo root directory. NOTE: this is only a vulnerability in environments that support multiple extensions, such as Apache with the mod_mime module enabled.	unknown 2008-06-17	7.5	CVE-2008-2742 MILW0RM OTHER-REF
BASIC-CMS.de -- BASIC-CMS	SQL injection vulnerability in pages/index.php in BASIC-CMS allows remote attackers to execute arbitrary SQL commands via the page_id parameter.	unknown 2008-06-20	7.5	CVE-2008-2789 MILW0RM BID XF
black_ice -- annotation_software	Stack-based buffer overflow in BiAnno ActiveX Control (BiAnno.ocx) in Black Ice Software Annotation Plugin 10.95 allows remote attackers to execute arbitrary code via a long parameter to the AnnoSaveToTiff method.	unknown 2008-06-17	9.3	CVE-2008-2745 MILW0RM MILW0RM BID
CartKeeper -- CKGold Shopping Cart	SQL injection vulnerability in item.php in CartKeeper CKGold Shopping Cart 2.5 and 2.7 allows remote attackers to execute arbitrary SQL commands via the category_id parameter, a different vector than CVE-2007-4736.	unknown 2008-06-19	7.5	CVE-2008-2774 MILW0RM XF
Cisco -- Intrusion Prevention System	Unspecified vulnerability in Cisco Intrusion Prevention System (IPS) 5.x before 5.1(8)E2 and 6.x before 6.0(5)E2, when inline mode and jumbo Ethernet support are enabled, allows remote attackers to cause a denial of service (panic), and possibly bypass intended restrictions on network traffic, via a "specific series of jumbo Ethernet frames."	unknown 2008-06-18	7.8	CVE-2008-2060
citect -- citectscada citect -- citectfacilities	Stack-based buffer overflow in the ODBC server service in Citect CitectSCADA 6 and 7, and CitectFacilities 7, allows remote attackers to execute arbitrary code via a long string in the second application packet in a TCP session on port 20222.	unknown 2008-06-16	7.6	CVE-2008-2639 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF CERT-VN BID SECTRACK XF
Clip-Share -- ClipShare	SQL injection vulnerability in group_posts.php in ClipShare before 3.0.1 allows remote attackers to execute arbitrary SQL commands via the tid parameter.	unknown 2008-06-20	7.5	CVE-2008-2793 MILW0RM BID XF
Drupal -- magic_tabs_module	The Magic Tabs module 5.x before 5.x-1.1 for Drupal allows remote attackers to execute arbitrary PHP code via unspecified URL arguments, possibly related to a missing "whitelist of callbacks."	unknown 2008-06-18	7.5	CVE-2008-2772
DT Centrepiece -- DT Centrepiece	SQL injection vulnerability in search.asp in DT Centrepiece 4.0 allows remote attackers to execute arbitrary SQL commands via the searchFor parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-19	7.5	CVE-2008-2775
DZOIC -- Handshakes	SQL injection vulnerability in index.php in DZOIC Handshakes 3.5 allows remote attackers to execute arbitrary SQL commands via the fname parameter in a members search action.	unknown 2008-06-19	7.5	CVE-2008-2781 BUGTRAQ BID XF
erocms.net -- eroCMS	SQL injection vulnerability in index.php in eroCMS 1.4 and earlier allows remote attackers to execute arbitrary SQL commands via the site parameter.	unknown 2008-06-20	7.5	CVE-2008-2792 MILW0RM BID

FreeCMS.us -- FreeCMS	SQL injection vulnerability in index.php in FreeCMS 0.2 allows remote attackers to execute arbitrary SQL commands via the page parameter.	unknown 2008-06-20	7.5	CVE-2008-2796 MILW0RM BID XF
FreeType -- FreeType	Integer overflow in FreeType2 before 2.3.6 allows context-dependent attackers to execute arbitrary code via a crafted set of 16-bit length values within the Private dictionary table in a Printer Font Binary (PFB) file, which triggers a heap-based buffer overflow.	unknown 2008-06-16	7.5	CVE-2008-1806 IDEFENSE OTHER-REF SECTRACK
FreeType -- FreeType	FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via an invalid "number of axes" field in a Printer Font Binary (PFB) file, which triggers a free of arbitrary memory locations, leading to memory corruption.	unknown 2008-06-16	7.5	CVE-2008-1807 IDEFENSE OTHER-REF BID SECTRACK
GlobalSCAPE -- CuteFTP	Directory traversal vulnerability in GlobalSCAPE CuteFTP Home 8.2.0 Build 02.26.2008.4 and CuteFTP Pro 8.2.0 Build 04.01.2008.1 allows remote FTP servers to create or overwrite arbitrary files via ..\ (dot dot backslash) sequences in responses to LIST commands, a related issue to CVE-2002-1345. NOTE: this can be leveraged for code execution by writing to a Startup folder.	unknown 2008-06-19	9.3	CVE-2008-2779 OTHER-REF SECTRACK XF
Gryphon -- gllcts2	SQL injection vulnerability in login.php in Gryphon gllcTS2 4.2.4 allows remote attackers to execute arbitrary SQL commands via the detail parameter.	unknown 2008-06-17	7.5	CVE-2008-2746 MILW0RM BID XF
Intel -- network_interface_controller	Unspecified vulnerability in the e1000g driver in Sun Solaris 10 and OpenSolaris before snv_93 allows remote attackers to cause a denial of service (network connectivity loss) via unknown vectors.	unknown 2008-06-16	7.8	CVE-2008-2707 SUNALERT BID SECTRACK
jamm-media -- jamm_cms	SQL injection vulnerability in index.php in JAMM CMS allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-18	7.5	CVE-2008-2755 MILW0RM BID
Kalptaru Infotech -- Comparison Engine Power Script	SQL injection vulnerability in product.detail.php in Kalptaru Infotech Comparison Engine Power Script 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-20	7.5	CVE-2008-2791 MILW0RM BID XF
Linux -- Kernel	The pppol2tp_recvmsg function in drivers/net/pppol2tp.c in the Linux kernel 2.6 before 2.6.26-rc6 allows remote attackers to cause a denial of service (kernel heap memory corruption and system crash) and possibly have unspecified other impact via a crafted PPPOL2TP packet that results in a large value for a certain length variable.	unknown 2008-06-18	7.8	CVE-2008-2750 OTHER-REF OTHER-REF SECTRACK XF
Menalto -- Gallery	Menalto Gallery before 2.2.5 allows remote attackers to bypass permissions for sub-albums via a ZIP archive.	unknown 2008-06-16	7.5	CVE-2008-2722 OTHER-REF
Microsoft -- Word	Microsoft Word 2000 9.0.2812 and 2003 11.8106.8172 does not properly handle unordered lists, which allows user-assisted remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted .doc file. NOTE: some of these details are obtained from third party information.	unknown 2008-06-18	7.1	CVE-2008-2752 OTHER-REF OTHER-REF OTHER-REF OTHER-REF BID
MountainGrafix -- easyTrade	SQL injection vulnerability in detail.php in MountainGrafix easyTrade 2.x allows remote attackers to execute arbitrary SQL commands via the id parameter.	unknown 2008-06-20	7.5	CVE-2008-2790 MILW0RM BID
Mozilla -- Firefox	Buffer overflow in Firefox 3.0 and 2.0.x has unknown impact and attack vectors. NOTE: due to lack of details as of 20080619, it is not clear whether this is the same issue as CVE-2008-2785. A CVE identifier has been assigned for tracking purposes.	unknown 2008-06-19	10.0	CVE-2008-2786 FULLDISC BID
mycrocms -- mycrocms	SQL injection vulnerability in index.php in MycroCMS 0.5, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the entry_id parameter.	unknown 2008-06-18	7.5	CVE-2008-2770 MILW0RM BID XF
NASM -- netwide_assembler NASM -- NASM	Off-by-one error in the ppscan function (preproc.c) in Netwide Assembler (NASM) 2.02 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted file that triggers a stack-based buffer overflow.	unknown 2008-06-16	9.3	CVE-2008-2719 OTHER-REF OTHER-REF MLIST MLIST
otomigenx -- otomigenx	Multiple directory traversal vulnerabilities in OtomiGenX 2.2 allow remote attackers to include and execute arbitrary local files via a .. (dot dot) in the lang parameter to (1) library_rss.php and (2) rss.php.	unknown 2008-06-19	7.5	CVE-2008-2782 MILW0RM OTHER-REF
phpRaider -- phpRaider	PHP remote file inclusion vulnerability in authentication/smf/smf.functions.php in Simple Machines phpRaider 1.0.6 and 1.0.7 allows remote attackers to execute arbitrary PHP code via a URL in the pConfig_auth[smf_path] parameter.	unknown 2008-06-18	7.5	CVE-2008-2769 BUGTRAQ OTHER-REF XF
pooya_site_builder -- 6.0	Multiple SQL injection vulnerabilities in Pooya Site Builder (PSB) 6.0 allow remote attackers to execute arbitrary SQL commands via the (1) xslIdn parameter to (a) utils/getXsl.aspx, and the (2) part parameter to (b) getXml.aspx and (c) getXls.aspx in utils/.	unknown 2008-06-18	7.5	CVE-2008-2753 BUGTRAQ MILW0RM OTHER-REF BID

RevokeSoft -- RevokeBB	SQL injection vulnerability in inc/class_search.php in the Search System in RevokeBB 1.0 RC11 allows remote attackers to execute arbitrary SQL commands via the search parameter.	unknown 2008-06-19	7.5	CVE-2008-2778 MILW0RM XF
Sun -- Java System Access Manager	Unspecified vulnerability in Sun Java System Access Manager (AM) 7.1, when used with certain versions and configurations of Sun Directory Server Enterprise Edition (DSEE), allows remote attackers to bypass authentication via unspecified vectors.	unknown 2008-06-16	9.3	CVE-2008-2705 SUNALERT BID XF
Sun -- one_calendar_server Sun -- Java System Calendar Server	Unspecified vulnerability in cshttpd in Sun Java System Calendar Server 6 and 6.3, and Sun ONE Calendar Server 6.0, when access logging (aka service.http.commandlog.all) is enabled, allows remote attackers to cause a denial of service (daemon crash) via unspecified vectors.	unknown 2008-06-18	10.0	CVE-2008-2749 BID SECUNIA XF
vim -- vim	Vim 7.1.314, 6.4, and other versions allows user-assisted remote attackers to execute arbitrary commands via Vim scripts that do not properly sanitize inputs before invoking the execute or system functions, as demonstrated using (1) filetype.vim, (2) zipplugin, (3) xpm.vim, (4) gzip_vim, and (5) netrw.	unknown 2008-06-16	9.3	CVE-2008-2712 BUGTRAQ BUGTRAQ OTHER-REF MLIST
x -- x11	The (1) SProcRecordCreateContext and (2) SProcRecordRegisterClients functions in the Record extension and the (3) SProcSecurityGenerateAuthorization function in the Security extension in the X server 1.4 in X.Org X11R7.3 allow context-dependent attackers to execute arbitrary code via requests with crafted length values that specify an arbitrary number of bytes to be swapped on the heap, which triggers heap corruption.	unknown 2008-06-16	9.0	CVE-2008-1377 IDEFENSE MLIST OTHER-REF REDHAT REDHAT SUNALERT SECTRACK
x -- x11	Integer overflow in the AllocateGlyph function in the Render extension in the X server 1.4 in X.Org X11R7.3 allows context-dependent attackers to execute arbitrary code via unspecified request fields that are used to calculate a heap buffer size, which triggers a heap-based buffer overflow.	unknown 2008-06-16	9.0	CVE-2008-2360 IDEFENSE SUNALERT UBUNTU SECTRACK
x -- x11	Multiple integer overflows in the Render extension in the X server 1.4 in X.Org X11R7.3 allow context-dependent attackers to execute arbitrary code via a (1) SProcRenderCreateLinearGradient, (2) SProcRenderCreateRadialGradient, or (3) SProcRenderCreateConicalGradient request with an invalid field specifying the number of bytes to swap in the request data, which triggers heap memory corruption.	unknown 2008-06-16	9.0	CVE-2008-2362 IDEFENSE MLIST DEBIAN REDHAT SUNALERT SUSE UBUNTU SECTRACK
XIGLA -- Absolute Image Gallery XE	SQL injection vulnerability in gallery.asp in Xigla Absolute Image Gallery XE allows remote attackers to execute arbitrary SQL commands via the categoryid parameter in a viewimage action.	unknown 2008-06-18	7.5	CVE-2008-2765 BUGTRAQ OTHER-REF BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
Adobe -- Flex Adobe -- flex_builder	Multiple cross-site scripting (XSS) vulnerabilities in the Flex 3 History Management feature in Adobe Flex 3.0.1 SDK and Flex Builder 3, and generated applications, allow remote attackers to inject arbitrary web script or HTML via the anchor identifier to (1) client-side-detection-with-history/history/historyFrame.html, (2) express-installation-with-history/history/historyFrame.html, or (3) no-player-detection-with-history/history/historyFrame.html in templates/html-templates/. NOTE: Firefox 2.0 and possibly other browsers prevent exploitation.	unknown 2008-06-18	4.3	CVE-2008-2640 OTHER-REF SECTRACK
albinoloverats -- Anubis Plugin	The Anubis (aka Anubis+Ripe160) plugin before 1.3 for encrypt stores the unencrypted file's size in cleartext in the header of the encrypted file, which allows attackers to distinguish between encrypted data and random padding at the end of the encrypted file.	unknown 2008-06-19	6.4	CVE-2008-2780 OTHER-REF XF
Apache -- apache webserver TYPO3 -- TYPO3	TYPO3 4.0.x before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.2.1, uses an insufficiently restrictive default fileDenyPattern for Apache, which allows remote attackers bypass security restrictions and upload configuration files such as .htaccess, or conduct file upload attacks using multiple extensions.	unknown 2008-06-16	6.5	CVE-2008-2717 BUGTRAQ OTHER-REF OTHER-REF DEBIAN
BitTorrent -- BitTorrent uTorrent -- uTorrent	The Web UI interface in (1) BitTorrent before 6.0.3 build 8642 and (2) uTorrent before 1.8beta build 10524 allows remote attackers to cause a denial of service (application crash) via an HTTP request with a malformed Range header.	unknown 2008-06-16	4.3	CVE-2008-0071 BUGTRAQ SECTRACK
Clam Anti-Virus -- ClamAV	libclamav/petite.c in ClamAV before 0.93.1 allows remote attackers to cause a denial of service via a crafted Petite file that triggers an out-of-bounds read.	unknown 2008-06-16	5.0	CVE-2008-2713 MLIST OTHER-REF OTHER-REF BID
Drupal -- Drupal Drupal -- node_hierarchy_module	The Node Hierarchy module 5.x before 5.x-1.1 and 6.x before 6.x-1.0 for Drupal does not properly implement access checks, which allows remote attackers with "access content" permissions to bypass restrictions and modify the node hierarchy via unspecified attack vectors.	unknown 2008-06-18	5.0	CVE-2008-2771 XF

Drupal -- taxonomy_image_module	Cross-site scripting (XSS) vulnerability in the Taxonomy Image module 5.x before 5.x-1.3 and 6.x before 6.x-1.3, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-18	4.3	CVE-2008-2773
DT Centrepiece -- DT Centrepiece	Cross-site scripting (XSS) vulnerability in search.asp in DT Centrepiece 4.0 allows remote attackers to inject arbitrary web script or HTML via the searchFor parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-19	4.3	CVE-2008-2776 SECUNIA
efiction -- efiction	SQL injection vulnerability in toplists.php in eFiction 3.0 and 3.4.3, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the list parameter.	unknown 2008-06-18	6.8	CVE-2008-2754 MILW0RM BID XF
Fetchmail -- Fetchmail	fetchmail 6.3.8 and earlier, when running in -v -v mode, allows remote attackers to cause a denial of service (crash and persistent mail failure) via a malformed mail message with long headers, which is not properly handled when using vsnprintf to format log messages.	unknown 2008-06-16	4.3	CVE-2008-2711 MLIST OTHER-REF
Horde -- Kronolith Horde -- Groupware Webmail Edition Horde -- Groupware	Multiple cross-site scripting (XSS) vulnerabilities in Horde Groupware, Groupware Webmail Edition, and Kronolith allow remote attackers to inject arbitrary web script or HTML via the timestamp parameter to (1) week.php, (2) workweek.php, and (3) day.php; and (4) the horde parameter in the PATH_INFO to the default URI. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-19	4.3	CVE-2008-2783 BID XF
IBM -- OS_400	Buffer overflow in the BrSmRcvAndCheck function in the RCHMGR module on IBM OS/400 V5R4M0, V5R4M5, and V6R1M0 allows local users to cause a denial of service (task halt and main storage dump) via unspecified vectors involving the running of diagnostics on a modem port. NOTE: there might be limited attack scenarios.	unknown 2008-06-16	4.7	CVE-2008-2709 AIXAPAR BID
IDM Computer Solutions Inc -- UltraEdit	Directory traversal vulnerability in the FTP and SFTP clients in IDM Computer Solutions Inc UltraEdit 14.00b allows remote FTP servers to create or overwrite arbitrary files via a .. (dot dot) or a ..\ (dot dot backslash) in a response to a LIST command.	unknown 2008-06-20	5.0	CVE-2008-2795 OTHER-REF BID SECUNIA
Luca Corbo -- Ortro	Cross-site scripting (XSS) vulnerability in Ortro before 1.3.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-19	4.3	CVE-2008-2777 OTHER-REF
ManageEngine -- OpUtils	Cross-site scripting (XSS) vulnerability in MainLayout.do in ManageEngine OpUtils 5.0 allows remote attackers to inject arbitrary web script or HTML via the hostName parameter, when viewing an SNMP graph. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2008-06-20	4.3	CVE-2008-2797 BID XF
Menalto -- Gallery	Cross-site scripting (XSS) vulnerability in Menalto Gallery before 2.2.5 allows remote attackers to inject arbitrary web script or HTML via the (1) host and (2) path components of a URL.	unknown 2008-06-16	4.3	CVE-2008-2720 OTHER-REF
Menalto -- Gallery	Unspecified vulnerability in the album-select module in Menalto Gallery before 2.2.5 allows remote attackers to obtain titles of hidden albums by attempting to add a new album to a hidden album.	unknown 2008-06-16	5.0	CVE-2008-2721
Menalto -- Gallery	embed.php in Menalto Gallery before 2.2.5 allows remote attackers to obtain the full path via unknown vectors related to "spoofing the remote address."	unknown 2008-06-16	5.0	CVE-2008-2723 OTHER-REF
Menalto -- Gallery	Menalto Gallery before 2.2.5 does not enforce permissions for non-album items that have been protected by a password, which might allow remote attackers to bypass intended access restrictions.	unknown 2008-06-16	5.0	CVE-2008-2724 OTHER-REF
Mozilla -- Firefox	Unspecified vulnerability in Firefox 3.0 and 2.0.x has unknown impact and remote attack vectors, aka ZDI-CAN-349.	unknown 2008-06-19	6.8	CVE-2008-2785 OTHER-REF BID SECUNIA
Novell -- eDirectory	Cross-site scripting (XSS) vulnerability in the iMonitor interface in Novell eDirectory 8.7.3.x before 8.7.3 sp10, and 8.8.x before 8.8.2 ftf2, allows remote attackers to inject arbitrary web script or HTML via unspecified parameters that are used within "error messages of the HTTP stack."	unknown 2008-06-18	4.3	CVE-2008-0925 OTHER-REF BID
OpenDocMan -- OpenDocMan	Cross-site scripting (XSS) vulnerability in out.php in OpenDocMan 1.2.5 allows remote attackers to inject arbitrary web script or HTML via the last_message parameter.	unknown 2008-06-20	4.3	CVE-2008-2787 BUGTRAQ OTHER-REF SECTRACK XF
OpenDocMan -- OpenDocMan	Cross-site scripting (XSS) vulnerability in index.php in OpenDocMan 1.2.5 allows remote attackers to inject arbitrary web script or HTML via the redirection parameter.	unknown 2008-06-20	4.3	CVE-2008-2788 OTHER-REF
OpenOffice -- OpenOffice	Untrusted search path vulnerability in a certain Red Hat build script for OpenOffice.org (OOo) 1.1.x on Red Hat Enterprise Linux (RHEL) 3 and 4 allows local users to gain privileges via a malicious library in the current working directory, related to incorrect quoting of the ORIGIN symbol for use in the RPATH library path.	unknown 2008-06-16	4.4	CVE-2008-2366 OTHER-REF REDHAT BID SECTRACK
Opera Software -- Opera	Opera before 9.26 allows remote attackers to misrepresent web page addresses using "certain characters" that "cause the page address text to be misplaced."	unknown 2008-06-16	5.0	CVE-2008-2714 OTHER-REF OTHER-REF OTHER-REF
Opera Software -- Opera	Unspecified vulnerability in Opera before 9.5 allows remote attackers to read cross-domain images via HTML CANVAS elements that use the images as patterns.	unknown 2008-06-16	5.0	CVE-2008-2715 OTHER-REF OTHER-REF BID

Opera Software -- Opera	Unspecified vulnerability in Opera before 9.5 allows remote attackers to spoof the contents of trusted frames on the same parent page by modifying the location, which can facilitate phishing attacks.	unknown 2008-06-16	5.0	CVE-2008-2716 OTHER-REF OTHER-REF OTHER-REF
PHP -- PHP	Directory traversal vulnerability in the posix_access function in PHP 5.2.6 and earlier allows remote attackers to bypass safe_mode restrictions via a .. (dot dot) in an http URL, which results in the URL being canonicalized to a local filename after the safe_mode check has successfully run.	unknown 2008-06-19	5.0	CVE-2008-2665 SREASONRES BID
PHP -- PHP	Multiple directory traversal vulnerabilities in PHP 5.2.6 and earlier allow context-dependent attackers to bypass safe_mode restrictions by creating a subdirectory named http: and then placing ../ (dot dot slash) sequences in an http URL argument to the (1) chdir or (2) ftok function.	unknown 2008-06-19	5.0	CVE-2008-2666 SREASONRES BID
Skulltag Team -- Skulltag	Skulltag 0.97d2-RC2 and earlier allows remote attackers to cause a denial of service (daemon hang) via a series of long, malformed connect packets, related to these packets being "parsed multiple times."	unknown 2008-06-18	5.0	CVE-2008-2748 BUGTRAQ OTHER-REF OTHER-REF BID
spamdyke -- spamdyke	The smtp_filter function in spamdyke before 3.1.8 does not filter RCPT commands after encountering the first DATA command, which allows remote attackers to use the server as an open mail relay by sending RCPT commands with invalid recipients, followed by a DATA command, followed by arbitrary RCPT commands and a second DATA command.	unknown 2008-06-19	6.4	CVE-2008-2784 OTHER-REF
Sun -- Solaris	Unspecified vulnerability in the event port implementation in Sun Solaris 10 allows local users to cause a denial of service (panic) by submitting and retrieving user-defined events, probably related to a NULL dereference.	unknown 2008-06-16	4.9	CVE-2008-2706 SUNALERT BID XF
Sun -- opensolaris Sun -- Solaris	Unspecified vulnerability in the Sun (1) UltraSPARC T2 and (2) UltraSPARC T2+ kernel modules in Sun Solaris 10, and OpenSolaris before snv_93, allows local users to cause a denial of service (panic) via unspecified vectors, probably related to core files.	unknown 2008-06-16	4.9	CVE-2008-2708 SUNALERT BID XF
Sun -- opensolaris Sun -- Solaris	Integer signedness error in the ip_set_srcfilter function in the IP Multicast Filter in uts/common/inet/ip/ip_multi.c in the kernel in Sun Solaris 10 and OpenSolaris before snv_92 allows local users to execute arbitrary code in other Solaris Zones via an SIOCSIPMSFILTER IOCTL request with a large value of the imsf->imsf_numsrc field, which triggers an out-of-bounds write of kernel memory. NOTE: this was reported as an integer overflow, but the root cause involves the bypass of a signed comparison.	unknown 2008-06-16	4.6	CVE-2008-2710 OTHER-REF SUNALERT BID
Sun -- Java System Application Server Sun -- glassfish	Multiple cross-site scripting (XSS) vulnerabilities in the Glassfish webadmin interface in Sun Java System Application Server 9.1_01 allow remote attackers to inject arbitrary web script or HTML via the (1) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:jndiProp:JndiNew, (2) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:resTypeProp:resType, (3) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:factoryClassProp:factoryClass, or (4) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:descProp:desc parameter to (a) resourceNode/customResourceNew.jsf; the (5) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:jndiProp:JndiNew, (6) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:resTypeProp:resType, (7) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:factoryClassProp:factoryClass, (8) propertyForm:propertyContentPage:prop! ertySheet:propertSectionTextField:jndiLookupProp:jndiLookup, or (9) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:descProp:desc parameter to (b) resourceNode/externalResourceNew.jsf; the (10) propertyForm:propertySheet:propertSectionTextField:jndiProp:Jndi, (11) propertyForm:propertySheet:propertSectionTextField:nameProp:name, or (12) propertyForm:propertySheet:propertSectionTextField:descProp:desc parameter to (c) resourceNode/jmsDestinationNew.jsf; the (13) propertyForm:propertySheet:generalPropertySheet:jndiProp:Jndi or (14) propertyForm:propertySheet:generalPropertySheet:descProp:cd parameter to (d) resourceNode/jmsConnectionNew.jsf; the (15) propertyForm:propertySheet:propertSectionTextField:jndiProp:jnditext or (16) propertyForm:propertySheet:propertSectionTextField:descProp:desc parameter to (e) resourceNode/jdbcResourceNew.jsf; the (17) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:nameProp:name, (18) propertyForm:pr! opertyContentPage:propertySheet:propertSectionTextField:classN! ameProp:classname, or (19) propertyForm:propertyContentPage:propertySheet:propertSectionTextField:loadOrderProp:loadOrder parameter to (f) applications/lifecycleModulesNew.jsf; or the (20) propertyForm:propertyContentPage:propertySheet:generalPropertySheet:jndiProp:name, (21) propertyForm:propertyContentPage:propertySheet:generalPropertySheet:resTypeProp:resType, or (22) propertyForm:propertyContentPage:propertySheet:generalPropertySheet:dbProp:db parameter to (g) resourceNode/jdbcConnectionPoolNew1.jsf.	unknown 2008-06-18	4.3	CVE-2008-2751 BUGTRAQ BID
Symantec -- Altiris Notification Server	Unspecified vulnerability in the GUI in Symantec Altiris Notification Server Agent 6.x before 6.0 SP3 R8 allows local users to gain privileges via unknown attack vectors.	unknown 2008-06-20	6.8	CVE-2008-2794 BID SECTRACK
TorrentTrader -- TorrentTrader Classic	Multiple SQL injection vulnerabilities in TorrentTrader 1.08 Classic allow remote attackers to execute arbitrary SQL commands via the (1) email or (2) wantusername parameter to account-signup.php, or the (3) receiver parameter to account-inbox.php in a msg action.	unknown 2008-06-18	6.8	CVE-2008-2428 OTHER-REF
TYPO3 -- TYPO3	Cross-site scripting (XSS) vulnerability in fe_adminlib.inc in TYPO3 4.0.x before 4.0.9, 4.1.x before 4.1.7, and 4.2.x before 4.2.1, as used in extensions such as (1) direct_mail_subscription, (2) feuser_admin, and (3) kb_md5fepw, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	unknown 2008-06-16	4.3	CVE-2008-2718 BUGTRAQ OTHER-REF DEBIAN

vbulletin -- vbulletin	Cross-site scripting (XSS) vulnerability in vBulletin 3.6.10 and 3.7.1 allows remote attackers to inject arbitrary web script or HTML via unknown vectors and an "obscure method." NOTE: the vector is probably in the redirect parameter to the Admin Control Panel (admincp/index.php).	unknown 2008-06-17	6.8	CVE-2008-2744 BUGTRAQ OTHER-REF BID
x -- x11	Integer overflow in the fbShmPutImage function in the MIT-SHM extension in the X server 1.4 in X.Org X11R7.3 allows context-dependent attackers to read arbitrary process memory via crafted values for a Pixmap width and height.	unknown 2008-06-16	6.8	CVE-2008-1379 IDEFENSE MLIST DEBIAN REDHAT REDHAT REDHAT SUNALERT SUSE UBUNTU FRSIRT FRSIRT SECTRACK XF
x -- x11	Integer overflow in the ProcRenderCreateCursor function in the Render extension in the X server 1.4 in X.Org X11R7.3 allows context-dependent attackers to cause a denial of service (daemon crash) via unspecified request fields that are used to calculate a glyph buffer size, which triggers a dereference of unmapped memory.	unknown 2008-06-16	4.0	CVE-2008-2361 IDEFENSE MLIST DEBIAN REDHAT REDHAT SUNALERT SUSE UBUNTU SECTRACK
Xerox -- xerox_4110 Xerox -- xerox_4590 Xerox -- xerox_4595	Cross-site scripting (XSS) vulnerability in the embedded web server in Xerox 4110, 4590, and 4595 Copier/Printers allows remote attackers to inject arbitrary web script or HTML via unknown attack vectors.	unknown 2008-06-17	4.3	CVE-2008-2743 OTHER-REF BID
XIGLA -- absolute_control_panel_xe	Cross-site scripting (XSS) vulnerability in admin/users.asp in Xigla Absolute Control Panel XE 1.0 allows remote attackers to inject arbitrary web script or HTML via the name parameter and other unspecified parameters. NOTE: some of these details are obtained from third party information.	unknown 2008-06-18	4.3	CVE-2008-2756 BUGTRAQ OTHER-REF BID
XIGLA -- absolute_news_manager_xe	SQL injection vulnerability in search.asp in Xigla Absolute News Manager XE 3.2 allows remote authenticated administrators to execute arbitrary SQL commands via the orderby parameter.	unknown 2008-06-18	6.5	CVE-2008-2757 BUGTRAQ OTHER-REF BID
XIGLA -- absolute_form_processor_xe	Multiple cross-site scripting (XSS) vulnerabilities in Xigla Absolute Form Processor XE 4.0 allow remote attackers to inject arbitrary web script or HTML via the (1) showfields, (2) text, and (3) submissions parameters to search.asp and the (4) name parameter to users.asp. NOTE: some of these details are obtained from third party information.	unknown 2008-06-18	4.3	CVE-2008-2759 BUGTRAQ OTHER-REF BID
XIGLA -- absolute_banner_manager	SQL injection vulnerability in searchbanners.asp in Xigla Absolute Banner Manager XE 2.0 allows remote authenticated administrators to execute arbitrary SQL commands via the orderby parameter.	unknown 2008-06-18	6.5	CVE-2008-2760 BUGTRAQ OTHER-REF BID
XIGLA -- absolute_form_processor_xe	SQL injection vulnerability in search.asp in Xigla Absolute Form Processor XE 4.0 allows remote authenticated administrators s to execute arbitrary SQL commands via the orderby parameter.	unknown 2008-06-18	6.5	CVE-2008-2762 BUGTRAQ OTHER-REF BID
XIGLA -- Absolute Live Support XE	SQL injection vulnerability in search.asp in Xigla Absolute Live Support XE 5.1 allows remote authenticated administrators to execute arbitrary SQL commands via the orderby parameter.	unknown 2008-06-18	6.5	CVE-2008-2763 BUGTRAQ OTHER-REF BID
XIGLA -- Absolute Image Gallery XE	Cross-site scripting (XSS) vulnerability in Xigla Absolute Image Gallery XE allows remote attackers to inject arbitrary web script or HTML via unspecified vectors in (1) admin/search.asp and (2) gallery.asp.	unknown 2008-06-18	4.3	CVE-2008-2766 BUGTRAQ OTHER-REF BID
XIGLA -- Absolute Poll Manager XE	SQL injection vulnerability in search.asp in Xigla Poll Manager XE allows remote authenticated users with administrator role privileges to execute arbitrary SQL commands via the orderby parameter.	unknown 2008-06-18	6.5	CVE-2008-2767 BUGTRAQ OTHER-REF BID

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
FreeType -- FreeType	Multiple off-by-one errors in FreeType2 before 2.3.6 allow context-dependent attackers to execute arbitrary code via (1) a crafted table in a Printer Font Binary (PFB) file or (2) a crafted SHC instruction in a TrueType Font (TTF) file, which triggers a heap-based buffer overflow.	unknown 2008-06-16	0.0	CVE-2008-1808 IDEFENSE OTHER-REF FRSIRT SECTRACK SECUNIA

no-ip -- dynamic_update_client	No-IP Dynamic Update Client (DUC) 2.2.1 on Windows uses weak permissions for the HKLM\SOFTWARE\Vitalwerks\DUC registry key, which allows local users to obtain obfuscated passwords and other sensitive information by reading the (1) TrayPassword, (2) Username, (3) Password, and (4) Hosts registry values.	unknown 2008-06-18	2.1	CVE-2008-2747 BUGTRAQ BID
XIGLA -- absolute_news_manager_xe	Multiple cross-site scripting (XSS) vulnerabilities in Xigla Absolute News Manager XE 3.2 allow remote authenticated administrators to inject arbitrary web script or HTML via the (1) pblname and (2) text parameters to (a) admin/search.asp, (3) name parameter to (b) admin/publishers.asp, and other unspecified vectors to (c) anmviewer.asp and (d) editarticleX.asp in admin/. NOTE: some of these details are obtained from third party information.	unknown 2008-06-18	3.5	CVE-2008-2758 BUGTRAQ OTHER-REF BID
XIGLA -- absolute_banner_manager	Multiple cross-site scripting (XSS) vulnerabilities in Xigla Absolute Banner Manager XE 2.0 allow remote authenticated administrators to inject arbitrary web script or HTML via the text parameter in (1) searchbanners.asp and (2) listadvertisers.asp, and other unspecified fields. NOTE: some of these details are obtained from third party information.	unknown 2008-06-18	3.5	CVE-2008-2761 BUGTRAQ OTHER-REF BID
XIGLA -- Absolute Live Support XE	Cross-site scripting (XSS) vulnerability in admin/search.asp in Xigla Absolute Live Support XE 5.1 allows remote authenticated administrators to inject arbitrary web script or HTML via unspecified vectors ("all fields").	unknown 2008-06-18	3.5	CVE-2008-2764 BUGTRAQ OTHER-REF BID
XIGLA -- Absolute Poll Manager XE	Cross-site scripting (XSS) vulnerability in admin/search.asp in Xigla Poll Manager XE allows remote authenticated users with administrator role privileges to inject arbitrary web script or HTML via unspecified vectors ("all fields").	unknown 2008-06-18	3.5	CVE-2008-2768 BUGTRAQ OTHER-REF BID

Back to top