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	Published	CVSS Score	Source & Patch Info
activecampaign -- triolive	SQL injection vulnerability in department_offline_context.php in ActiveCampaign TrioLive before 1.58.7 allows remote attackers to execute arbitrary SQL commands via the department_id parameter to index.php.	2008-11-13	7.5	CVE-2008-505 FRSIRT SECUNIA CONFIRM
adobe -- flash_player	Unspecified vulnerability in the Flash Player ActiveX control in Adobe Flash Player 9.0.124.0 and earlier on Windows allows attackers to obtain sensitive information via unknown vectors.	2008-11-10	7.1	CVE-2008-482 BID CONFIRM
adobe -- coldfusion	Unspecified vulnerability in Adobe ColdFusion 8 and 8.0.1 and ColdFusion MX 7.0.2 allows local users to bypass sandbox restrictions, and obtain sensitive information or possibly gain privileges, via unknown vectors.	2008-11-10	7.2	CVE-2008-483 CONFIRM
agaresmedia -- themesitescript	PHP remote file inclusion vulnerability in upload/admin/frontpage_right.php in Agares Media ThemeSiteScript 1.0 allows remote attackers to execute arbitrary PHP code via a URL in the loadadminpage parameter.	2008-11-13	10.0	CVE-2008-506 BID MILW0RM
aspindir -- dizi_portali	SQL injection vulnerability in film.asp in Yigit Aybuga Dizi Portali allows remote attackers to execute arbitrary SQL commands via the film parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-13	7.5	CVE-2008-505 XF MISC BID SECUNIA
clam_anti-virus -- clamav	Off-by-one error in the get_unicode_name function (libclamav/vba_extract.c) in Clam Anti-Virus	2008-11-12	9.3	CVE-2008-505 BID

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	(ClamAV) before 0.94.1 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted VBA project file, which triggers a heap-based buffer overflow.			
deeserver -- panuwat_promoteweb_mysql	SQL injection vulnerability in go.php in Panuwat PromoteWeb MySQL, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-11-14	7.5	CVE-2008-506 XF BID MILW0RM
develop_it_easy -- membership_system	Multiple SQL injection vulnerabilities in Develop It Easy Membership System 1.3 allow remote attackers to execute arbitrary SQL commands via the (1) email and (2) password parameters to customer_login.php and the (3) user_name and (4) user_pass parameters to admin/index.php. NOTE: some of these details are obtained from third party information.	2008-11-13	7.5	CVE-2008-505 XF BID SECUNIA MILW0RM
easy-script -- tlguesbook	TlGuestBook 1.2 allows remote attackers to bypass authentication and gain administrative access by setting the tlGuestBook_login cookie to admin.	2008-11-13	7.5	CVE-2008-506 BID MILW0RM
elkagroup -- image_gallery	SQL injection vulnerability in view.php in ElkaGroup Image Gallery 1.0 allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2008-11-12	7.5	CVE-2008-503 BID SECUNIA MISC
graphiks -- myforum	Graphiks MyForum 1.3 allows remote attackers to bypass authentication and gain administrative access by setting the (1) myforum_login and (2) myforum_pass cookies to 1.	2008-11-12	7.5	CVE-2008-504 XF BID MILW0RM
h&h -- websoccer	SQL injection vulnerability in liga.php in H&H WebSoccer 2.80 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2008-11-13	7.5	CVE-2008-506 BID SECUNIA MISC
hp -- tru64	Unspecified vulnerability in the AdvFS showfile command in HP Tru64 UNIX 5.1B-3 and 5.1B-4 allows local users to gain privileges via unspecified vectors.	2008-11-07	7.2	CVE-2008-44 BID
isecsoft -- anti-trojan_elite	Buffer overflow in Atepmon.sys in ISecSoft Anti-Trojan Elite 4.2.1 and earlier, and possibly 4.2.2, allows local users to cause a denial of service (crash) and possibly execute arbitrary code via long inputs to the 0x00222494 IOCTL.	2008-11-12	7.2	CVE-2008-504 BID MISC SECUNIA
isecsoft -- anti-keylogger_elite	Buffer overflow in AKEProtect.sys 3.3.3.0 in ISecSoft Anti-Keylogger Elite 3.3.0 and earlier, and possibly other versions including 3.3.3, allows local users to gain privileges via long inputs to the (1) 0x002224A4, (2) 0x002224C0, and (3) 0x002224CC IOCTL.	2008-11-12	7.2	CVE-2008-504 BID MISC MILW0RM SECUNIA
jooblog -- jooblog	SQL injection vulnerability in the JooBlog (com_jb2) component 0.1.1 for Joomla! allows remote attackers to execute arbitrary SQL commands via the PostID parameter to index.php.	2008-11-12	7.5	CVE-2008-505 BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
joomla -- com_rssreader	PHP remote file inclusion vulnerability in admin.rssreader.php in the Simple RSS Reader (com_rssreader) 1.0 component for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_live_site parameter.	2008-11-13	10.0	CVE-2008-505 BID MILW0RM FRSIRT
libcaudio -- libcaudio	Heap-based buffer overflow in the cddb_read_disc_data function in cddb.c in libcdaudio 0.99.12p2 allows remote attackers to execute arbitrary code via long CDDB data.	2008-11-10	10.0	CVE-2008-503 BID MLIST MLIST MISC
linux -- kernel	The chip_command function in drivers/media/video/tvaudio.c in the Linux kernel 2.6.25.x before 2.6.25.19, 2.6.26.x before 2.6.26.7, and 2.6.27.x before 2.6.27.3 allows attackers to cause a denial of service (NULL function pointer dereference and OOPS) via unknown vectors.	2008-11-10	7.8	CVE-2008-503 BID
microsoft -- windows	Microsoft Windows 2000 Gold through SP4, XP Gold through SP3, Server 2003 SP1 and SP2, Vista Gold and SP1, and Server 2008 allows remote SMB servers to execute arbitrary code on a client machine by replaying the NTLM credentials of a client user, as demonstrated by backrush, aka "SMB Credential Reflection Vulnerability."	2008-11-12	9.3	CVE-2008-403 BID MS
modernbill -- modernbill	Multiple PHP remote file inclusion vulnerabilities in ModernBill 4.4 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the DIR parameter to (1) export_batch.inc.php, (2) run_auto_suspend.cron.php, and (3) send_email_cache.php in include/scripts/; (4) include/misc/mod_2checkout/2checkout_return.inc.php; and (5) include/html/nettools.popup.php, different vectors than CVE-2006-4034 and CVE-2005-1054.	2008-11-13	10.0	CVE-2008-506 XF MILW0RM SECUNIA
mole_group -- pizza_script	SQL injection vulnerability in index.php in Mole Group Pizza Script allows remote attackers to execute arbitrary SQL commands via the manufacturers_id parameter.	2008-11-12	7.5	CVE-2008-504 XF BID MILW0RM SECUNIA
mole_group -- rental_script	SQL injection vulnerability in admin/index.php in Mole Group Rental Script allows remote attackers to execute arbitrary SQL commands via the username parameter.	2008-11-12	7.5	CVE-2008-504 BID MILW0RM SECUNIA
mozilla -- firefox mozilla -- seamonkey	The http-index-format MIME type parser (nsDirIndexParser) in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 does not check for an allocation failure, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an HTTP index response with a crafted 200 header, which triggers memory corruption and a buffer overflow.	2008-11-13	7.5	CVE-2008-00 MISC CONFIRM

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox 2.x before 2.0.0.18 and SeaMonkey 1.x before 1.1.13 do not properly check when the Flash module has been dynamically unloaded properly, which allows remote attackers to execute arbitrary code via a crafted SWF file that "dynamically unloads itself from an outside JavaScript function," which triggers an access of an expired memory address.	2008-11-13	9.3	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	jslock.cpp in Mozilla Firefox 3.x before 3.0.2, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by modifying the window.__proto__.__proto__ object in a way that causes a lock on a non-native object, which triggers an assertion failure related to the OBJ_IS_NATIVE function.	2008-11-13	10.0	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Integer overflow in xpcom/io/nsEscape.cpp in the browser engine in Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via unknown vectors.	2008-11-13	10.0	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The JavaScript engine in Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via vectors related to "insufficient class checking" in the Date class.	2008-11-13	10.0	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	nsFrameManager in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by modifying properties of a file input element while it is still being initialized, then using the blur method to access uninitialized memory.	2008-11-13	9.3	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The nsXMLHttpRequest::NotifyEventListeners method in Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to bypass the same-origin policy and execute arbitrary script via multiple listeners, which bypass the inner window check.	2008-11-13	7.5	CVE-2008-50 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey	Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to bypass the protection mechanism for codebase principals and execute arbitrary script via the -moz-binding CSS property in a signed JAR file.	2008-11-13	7.5	CVE-2008-50 MISC CONFIRM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 3.x before 3.0.4, Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 do not properly escape quote characters used for XML processing, allows remote attackers to conduct XML injection attacks via the default namespace in an E4X document.	2008-11-13	7.5	CVE-2008-502 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The AppendAttributeValue function in the JavaScript engine in Mozilla Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via unknown vectors that trigger memory corruption, as demonstrated by e4x/extensions/regress-410192.js.	2008-11-13	10.0	CVE-2008-505 MISC CONFIRM
network-client.com -- ftp_now	Heap-based buffer overflow in Network-Client FTP Now 2.6, and possibly other versions, allows remote FTP servers to cause a denial of service (crash) via a 200 server response that is exactly 1024 characters long.	2008-11-12	10.0	CVE-2008-504 BID MILW0RM
novell -- edirectory	Use after free vulnerability in the NetWare Core Protocol (NCP) feature in Novell eDirectory 8.7.3 SP10 before 8.7.3 SP10 FTF1 and 8.8 SP2 for Windows allows remote attackers to cause a denial of service and possibly execute arbitrary code via a sequence of "Get NCP Extension Information By Name" requests that cause one thread to operate on memory after it has been freed in another thread, which triggers memory corruption, aka Novell Bug 373852.	2008-11-12	10.0	CVE-2008-503 CONFIRM CONFIRM
novell -- zenworks_desktop_management	Heap-based buffer overflow in an ActiveX control in Novell ZENworks Desktop Management 6.5 allows remote attackers to execute arbitrary code via a long argument to the CanUninstall method.	2008-11-14	9.3	CVE-2008-507 XF BID BUGTRAQ
otmanager -- otmanager	PHP remote file inclusion vulnerability in Admin/ADM_Pagina.php in OTManager 2.4 allows remote attackers to execute arbitrary PHP code via a URL in the Tipo parameter.	2008-11-13	10.0	CVE-2008-506 BID MILW0RM
php-fusion -- freshlinks_module	SQL injection vulnerability in index.php in the Freshlinks 1.0 RC1 module for PHP-Fusion allows remote attackers to execute arbitrary SQL commands via the linkid parameter.	2008-11-14	7.5	CVE-2008-501 XF BID MILW0RM
preproject -- pre_simple_cms	SQL injection vulnerability in siteadmin/loginsucess.php in Pre Simple CMS allows remote attackers to execute arbitrary SQL commands via the user parameter, as reachable from siteadmin/adminlogin.php. NOTE: some of these details are obtained from third party information.	2008-11-13	7.5	CVE-2008-505 FRSIRT SECUNIA OSVDB MILW0RM
pro_chat_rooms -- pro_chat_rooms	SQL injection vulnerability in Pro Chat Rooms 3.0.3, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the gud parameter to (1) index.php and (2) admin.php.	2008-11-14	7.5	CVE-2008-501 BID MILW0RM

Back to top

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
python_software_foundation -- python	Multiple integer overflows in Python 2.5.2 allow context-dependent attackers to have an unknown impact via a large integer value in the tabsize argument to the expandtabs method, as implemented by (1) the string_expandtabs function in Objects/stringobject.c and (2) the unicode_expandtabs function in Objects/unicodeobject.c. NOTE: this vulnerability reportedly exists because of an incomplete fix for CVE-2008-2315.	2008-11-10	10.0	CVE-2008-50 MLIST MLIST CONFIRM CONFIRM CONFIRM MISC
sap -- sapgui simba_technologies -- mdrmsap_activex_control	Unspecified vulnerability in the Simba MDrmSap ActiveX control in mdrmsap.dll in SAP SAPgui allows remote attackers to execute arbitrary code via unknown vectors involving instantiation by Internet Explorer.	2008-11-10	9.3	CVE-2008-43 CERT-VN XF BID FRSIRT OSVDB
sun -- opensolaris sun -- solaris	in.dhcpd in the DHCP implementation in Sun Solaris 8 through 10, and OpenSolaris before snv_103, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via unknown DHCP requests related to the "number of offers," aka Bug ID 6713805.	2008-11-10	10.0	CVE-2008-50 CONFIRM
sweex -- ro002_router	Sweex RO002 Router with firmware Ts03-072 has "rdc123" as its default password for the "rdc123" account, which makes it easier for remote attackers to obtain access. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-12	7.5	CVE-2008-50 XF BID SECUNIA
university_of_washington -- alpine university_of_washington -- imap_toolkit	Multiple stack-based buffer overflows in (1) University of Washington IMAP Toolkit 2002 through 2007c, (2) University of Washington Alpine 2.00 and earlier, and (3) Panda IMAP allow (a) local users to gain privileges by specifying a long folder extension argument on the command line to the tmail or dmail program; and (b) remote attackers to execute arbitrary code by sending e-mail to a destination mailbox name composed of a username and '+' character followed by a long string, processed by the tmail or possibly dmail program.	2008-11-10	10.0	CVE-2008-50 CONFIRM MLIST
videolan -- vlc_media_player	Stack-based buffer overflow in VideoLAN VLC media player 0.5.0 through 0.9.5 might allow user-assisted attackers to execute arbitrary code via the header of an invalid CUE image file, related to modules/access/vcd/cdrom.c. NOTE: this identifier originally included an issue related to RealText, but that issue has been assigned a separate identifier, CVE-2008-5036.	2008-11-10	9.3	CVE-2008-50 CONFIRM MISC MLIST MLIST MLIST CONFIRM
videolan -- vlc_media_player	Stack-based buffer overflow in VideoLAN VLC media player 0.9.x before 0.9.6 might allow user-assisted attackers to execute arbitrary code via an an invalid RealText (rt) subtitle file, related to the ParseRealText function in modules/demux/subtitle.c. NOTE: this issue	2008-11-10	9.3	CVE-2008-50 CONFIRM MISC MLIST MLIST

Back to top

High Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	was SPLIT from CVE-2008-5032 on 20081110.			MLIST CONFIRM
vmware -- esx vmware -- esxi	Directory traversal vulnerability in VMWare ESXi 3.5 before ESXe350-200810401-O-UG and ESX 3.5 before ESX350-200810201-UG allows administrators with the Datastore.FileManagement privilege to gain privileges via unknown vectors.	2008-11-10	9.3	CVE-2008-428 MLIST
yoxel -- yoxel	Multiple eval injection vulnerabilities in itpm_estimate.php in Yoxel 1.23beta and earlier allow remote authenticated users to execute arbitrary PHP code via the proj_id parameter.	2008-11-14	9.0	CVE-2008-507 BID MILW0RM
zeeways -- photovideotube	Zeeways PhotoVideoTube 1.1 and earlier allows remote attackers to bypass authentication and perform administrative tasks via a direct request to admin/home.php.	2008-11-12	7.5	CVE-2008-504 MILW0RM FRSIRT SECUNIA

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
a_mennucc1 -- printfilters-ppd	** DISPUTED ** master-filter in printfilters-ppd 2.13 allows local users to overwrite arbitrary files via a symlink attack on the /tmp/filter.debug temporary file. NOTE: the vendor disputes this vulnerability, stating 'this package does not have " possibility of attack with the help of symlinks"'.	2008-11-10	6.9	CVE-2008-5034 MISC MLIST MISC MISC
activecampaign -- triolive	Cross-site scripting (XSS) vulnerability in department_offline_context.php in ActiveCampaign TrioLive before 1.58.7 allows remote attackers to inject arbitrary web script or HTML via the department_id parameter to index.php.	2008-11-13	4.3	CVE-2008-5056 MISC CONFIRM
adobe -- flash_player	Cross-site scripting (XSS) vulnerability in Adobe Flash Player 9.0.124.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors involving HTTP response headers.	2008-11-10	4.3	CVE-2008-4818 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
adobe -- flash_player	Unspecified vulnerability in Adobe Flash Player 9.0.124.0 and earlier makes it easier for remote attackers to conduct DNS rebinding attacks via unknown vectors.	2008-11-10	6.8	CVE-2008-4819 BID CONFIRM
adobe -- flash_player	Adobe Flash Player 9.0.124.0 and earlier does not properly interpret policy files, which allows remote attackers to bypass a non-root domain policy.	2008-11-10	6.8	CVE-2008-4822 BID CONFIRM
adobe -- flash_player	Cross-site scripting (XSS) vulnerability in Adobe Flash Player 9.0.124.0 and earlier allows remote attackers to inject arbitrary web script or HTML via vectors related to loose interpretation of an ActionScript attribute.	2008-11-10	4.3	CVE-2008-4823 BID CONFIRM
gnu -- gnutls	The _gnutls_x509_verify_certificate function in lib/x509/verify.c in libgnutls in GnuTLS before 2.6.1 trusts certificate chains in which the last certificate is an arbitrary trusted, self-signed certificate, which allows man-in-the-middle attackers to insert a spoofed certificate for any Distinguished Name (DN).	2008-11-12	4.3	CVE-2008-4989 BID MLIST
htop -- htop	htop 0.7 writes process names to a terminal without sanitizing non-printable characters, which might allow local users to hide processes, modify arbitrary files, or have unspecified other impact via a process name with "crazy control strings."	2008-11-14	4.6	CVE-2008-5076 XF MLIST MLIST CONFIRM
ibm -- lotus	Multiple cross-site scripting (XSS) vulnerabilities in IBM Lotus Quickr 8.1 before 8.1.0.2 services for Lotus Domino allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly related to qpconfig_sample.xml, aka SPR CWIR7KMPVP and	2008-11-10	4.3	CVE-2008-5011 CONFIRM

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	THES7F9NVR, a different vulnerability than CVE-2008-2163 and CVE-2008-3860.			
ibm -- hardware_management_console	The Resource Monitoring and Control (RMC) daemon in IBM Hardware Management Console (HMC) 7 release 3.2.0 SP1 and 3.3.0 SP2 allows remote attackers to cause a denial of service (daemon crash or hang) via a packet with an invalid length.	2008-11-10	5.0	CVE-2008-5035 CONFIRM CONFIRM XF CONFIRM CONFIRM BID FRSIRT SECUNIA
k-lite -- mega_codec_pack	vsfilter.dll in K-Lite Mega Codec Pack 3.5.7.0 allows remote attackers to cause a denial of service (application crash) via a malformed FLV file.	2008-11-14	4.3	CVE-2008-5072 XF BID MILW0RM MISC
kkeim -- kmita_catalogue	Cross-site scripting (XSS) vulnerability in search.php in Kmita Catalogue 2.x allows remote attackers to inject arbitrary web script or HTML via the q parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-13	4.3	CVE-2008-5067 BID OSVDB SECUNIA
kkeim -- kmita_gallery	Multiple cross-site scripting (XSS) vulnerabilities in Kmita Gallery allow remote attackers to inject arbitrary web script or HTML via the (1) begin parameter to index.php and the (2) searchtext parameter to search.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2008-11-13	4.3	CVE-2008-5068 OSVDB OSVDB SECUNIA
linux -- kernel	The __scm_destroy function in net/core/scm.c in the Linux kernel 2.6.27.4, 2.6.26, and earlier makes indirect recursive calls to itself through calls to the fput function, which allows local users to cause a denial of service (panic) via vectors	2008-11-10	4.9	CVE-2008-5029 BID

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	related to sending an SCM_RIGHTS message through a UNIX domain socket and closing file descriptors.			
microsoft -- sharepoint	Microsoft SharePoint uses URLs with the same hostname and port number for a web site's primary files and individual users' uploaded files (aka attachments), which allows remote authenticated users to leverage same-origin relationships and conduct cross-site scripting (XSS) attacks by uploading HTML documents.	2008-11-10	4.3	CVE-2008-5026 MISC BUGTRAQ BUGTRAQ BUGTRAQ
microsoft -- internet_explorer	Cross-domain vulnerability in Microsoft XML Core Services 3.0 and 4.0, as used in Internet Explorer, allows remote attackers to obtain sensitive information from another domain via a crafted XML document, related to improper error checks for external DTDs, aka "MSXML DTD Cross-Domain Scripting Vulnerability."	2008-11-12	4.3	CVE-2008-4029 BID MS
microsoft -- 20007_office_system microsoft -- expression_web microsoft -- office microsoft -- office_compatibility_pack_for_word_excel_ppt_2007 microsoft -- office_groove_server microsoft -- office_sharepoint_server microsoft -- word_viewer	Cross-domain vulnerability in Microsoft XML Core Services 3.0 through 6.0, as used in Microsoft Expression Web, Office, Internet Explorer, and other products, allows remote attackers to obtain sensitive information from another domain and corrupt the session state via HTTP request header fields, as demonstrated by the Transfer-Encoding field, aka "MSXML Header Request Vulnerability."	2008-11-12	4.3	CVE-2008-4033 BID
microsoft -- windows_server_2003 microsoft -- windows_vista	Race condition in Microsoft Windows Server 2003 and Vista allows local users to cause a denial of service (crash or hang) via a multi-threaded application that makes many calls to UnhookWindowsHookEx while	2008-11-12	4.0	CVE-2008-5044 BID BUGTRAQ MISC

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	certain other desktop activity is occurring.			
modernbill -- modernbill	Cross-site scripting (XSS) vulnerability in index.php in ModernBill 4.4 and earlier allows remote attackers to inject arbitrary web script or HTML via a Javascript event in the new_language parameter in a login action.	2008-11-13	4.3	CVE-2008-5059 XF MILW0RM SECUNIA
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox 2.x before 2.0.0.18, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 do not properly change the source URI when processing a canvas element and an HTTP redirect, which allows remote attackers to bypass the same origin policy and access arbitrary images that are not directly accessible to the attacker. NOTE: this issue can be leveraged to enumerate software on the client by performing redirections related to moz-icon.	2008-11-13	5.0	CVE-2008-5012 MISC MISC CONFIRM
mozilla -- firefox	Mozilla Firefox 3.x before 3.0.4 assigns chrome privileges to a file: URI when it is accessed in the same tab from a chrome or privileged about: page, which makes it easier for user-assisted attackers to execute arbitrary JavaScript with chrome privileges via malicious code in a file that has already been saved on the local system.	2008-11-13	5.1	CVE-2008-5015 MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The layout engine in Mozilla Firefox 3.x before 3.0.4, Thunderbird 2.x before 2.0.0.18, and SeaMonkey 1.x before 1.1.13 allows remote attackers to cause a denial of service (crash) via multiple vectors that trigger an assertion failure or other consequences.	2008-11-13	5.0	CVE-2008-5016 MISC CONFIRM
mozilla -- firefox	The session restore feature in Mozilla Firefox 3.x before 3.0.4	2008-11-13	4.3	CVE-2008-5019 MISC

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	and 2.x before 2.0.0.18 allows remote attackers to violate the same origin policy to conduct cross-site scripting (XSS) attacks and execute arbitrary JavaScript with chrome privileges via unknown vectors.			CONFIRM
nagios -- nagios op5 -- monitor	The Nagios process in (1) Nagios before 3.0.5 and (2) op5 Monitor before 4.0.1 allows remote authenticated users to bypass authorization checks, and trigger execution of arbitrary programs by this process, via an (a) custom form or a (b) browser addon.	2008-11-10	6.5	CVE-2008-5027 BID MISC MLIST
nagios -- nagios op5 -- monitor	Cross-site request forgery (CSRF) vulnerability in cmd.cgi in (1) Nagios 3.0.5 and (2) op5 Monitor before 4.0.1 allows remote attackers to send commands to the Nagios process, and trigger execution of arbitrary programs by this process, via unspecified HTTP requests.	2008-11-10	6.8	CVE-2008-5028 CONFIRM MLIST
php-nuke -- league_module	Cross-site scripting (XSS) vulnerability in the League module for PHP-Nuke, possibly 2.4, allows remote attackers to inject arbitrary web script or HTML via the tid parameter in a team action to modules.php.	2008-11-12	4.3	CVE-2008-5039 BID BUGTRAQ
scriptsfrenzy -- e-uploader_pro	Multiple SQL injection vulnerabilities in E-Uploader Pro 1.0 (aka Uploader PRO), when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) id parameter to (a) img.php, (b) file.php, (c) mail.php, (d) thumb.php, (e) zip.php, and (f) zipit.php, and (2) the view parameter to (g) browser.php.	2008-11-14	6.8	CVE-2008-5075 BID MILW0RM
smolinari -- mini_web_calendar	Cross-site scripting (XSS) vulnerability in php/cal_default.php in Mini Web Calendar (mwcal) 1.2	2008-11-13	4.3	CVE-2008-5061 BID MILW0RM FRSIRT

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
	allows remote attackers to inject arbitrary web script or HTML via the URL.			SECUNIA OSVDB
smolinari -- mini_web_calendar	Directory traversal vulnerability in php/cal_pdf.php in Mini Web Calendar (mwcal) 1.2 allows remote attackers to read arbitrary files via directory traversal sequences in the thefile parameter.	2008-11-13	5.0	CVE-2008-5062 BID MILW0RM FRSIRT SECUNIA OSVDB
sun -- solstice_x.25	Race condition in the s_xout kernel module in Sun Solstice X.25 9.2, when running on a multiple CPU machine, allows local users to cause a denial of service (panic) via vectors involving reading the /dev/xty file.	2008-11-10	4.0	CVE-2008-5009 CONFIRM CONFIRM
vmware -- ace vmware -- esx vmware -- esxi vmware -- player vmware -- server vmware -- workstation	The CPU hardware emulation in VMware Workstation 6.0.5 and earlier and 5.5.8 and earlier; Player 2.0.x through 2.0.5 and 1.0.x through 1.0.8; ACE 2.0.x through 2.0.5 and earlier, and 1.0.x through 1.0.7; Server 1.0.x through 1.0.7; ESX 2.5.4 through 3.5; and ESXi 3.5, when running 32-bit and 64-bit guest operating systems, does not properly handle the Trap flag, which allows authenticated guest OS users to gain privileges on the guest OS.	2008-11-10	6.9	CVE-2008-4915 XF CONFIRM SECTRACK BID BUGTRAQ FRSIRT SECUNIA SECUNIA MLIST

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- flash_player	Adobe Flash Player 9.0.124.0 and earlier, when a Mozilla browser is used, does not properly interpret jar: URLs, which allows attackers to obtain sensitive information via unknown vectors.	2008-11-10	0.0	CVE-2008-4821 BID CONFIRM
ibm -- metrica_service_assurance_framework	Multiple cross-site scripting (XSS) vulnerabilities in the web-based interface in IBM Metrica Service Assurance Framework allow remote authenticated users to inject	2008-11-12	3.5	CVE-2008-5043 XF BID BUGTRAQ

Back to top

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	arbitrary web script or HTML via (1) the elementid parameter in a generatedreportresults action to the ReportTree program, (2) the jnlpname parameter to the Launch program, or (3) the :tasklabel parameter to the ReportRequest program, related to the name of a report.			FULLDISC

Back to top