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 (CVSS Score: 7.0 .. 10.0)				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
blogphp -- blogphp	index.php in BlogPHP 2.0 allows remote attackers to gain administrator privileges via a crafted email parameter in a register2 action.	2009-04-23	7.5	CVE-2008-6745 XF BID MILW0RM
china-on-site -- flexphpdirectory	Unrestricted file upload vulnerability in add.php in FlexPHPDirectory 0.0.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in photo/.	2009-04-24	7.5	CVE-2008-6750 XF MILW0RM SECUNIA OSVDB
clamav -- clamav	Stack-based buffer overflow in the cli_url_canon function in libclamav/phishcheck.c in ClamAV before 0.95.1 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted URL.	2009-04-23	10.0	CVE-2009-1372 VUPEN
creloaded -- cre_loaded	SQL injection vulnerability in product_info.php in CRE Loaded 6.2 allows remote attackers to execute arbitrary SQL commands via the products_id parameter.	2009-04-24	7.5	CVE-2009-1403 XF BID MILW0RM

dawningsoft -- powerchm	Stack-based buffer overflow in Dawningsoft PowerCHM 5.7 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via an HTML file with a link to a long URL, as demonstrated by a .rar URL.	2009-04-21	9.3	CVE-2009-1352 XF BID MILW0RM
debian -- apt	apt-get in apt before 0.7.21 does not check for the correct error code from gpgv, which causes apt to treat a repository as valid even when it has been signed with a key that has been revoked or expired, which might allow remote attackers to trick apt into installing malicious repositories.	2009-04-21	10.0	CVE-2009-1358 CONFIRM
ea -- crysis	Crysis 1.21 and earlier allows remote attackers to obtain sensitive player information such as real IP addresses by sending a keyexchange packet without a previous join packet, which causes Crysis to send a disconnect packet that includes unrelated log information.	2009-04-21	7.8	CVE-2008-6737 XF BID SECUNIA OSVDB MISC
elecard -- elecard_avc_hd_player	Stack-based buffer overflow in Elecard AVC HD Player allows remote attackers to execute arbitrary code via a long MP3 filename in a playlist (.xpl) file.	2009-04-21	9.3	CVE-2009-1356 BID MILW0RM
foolabs -- xpdf	Multiple buffer overflows in the JBIG2 MMR decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allow remote attackers to execute arbitrary code via a crafted PDF file.	2009-04-23	7.5	CVE-2009-1182 CONFIRM REDHAT SECUNIA
foolabs -- xpdf	Integer overflow in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, as used in Poppler and other products, when running on Mac OS X, has unspecified impact, related to "g*allocn."	2009-04-23	10.0	CVE-2009-0165 CONFIRM
gscripts -- dns_tools	dig.php in GScripts.net DNS Tools allows remote attackers to execute arbitrary commands via shell metacharacters in the host parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-22	10.0	CVE-2009-1361 SECUNIA
heikki_ylinen -- apollo	Heap-based buffer overflow in Apollo 37zz allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a long URI in a playlist (.m3u) file.	2009-04-21	9.3	CVE-2009-1351 BID MILW0RM

hp -- storageworks_storage_mirroring	Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to cause a denial of service or obtain "access" via unknown vectors.	2009-04-21	7.5	CVE-2009-0716 HP HP
hp -- storageworks_storage_mirroring	Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to execute arbitrary code via unknown vectors.	2009-04-21	10.0	CVE-2009-0718 HP HP
ibm -- aix	Stack-based buffer overflow in muxatmd in IBM AIX 5.2, 5.3, and 6.1 allows local users to gain privileges via a long filename.	2009-04-21	7.2	CVE-2009-1355 VUPEN BID
keller_web_admin -- kwa	Directory traversal vulnerability in Public/index.php in Keller Web Admin CMS 0.94 Pro allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the action parameter.	2009-04-21	7.5	CVE-2008-6734 XF BID MILW0RM MILW0RM
linux -- kernel	The __inet6_check_established function in net/ipv6/inet6_hashtables.c in the Linux kernel before 2.6.29, when Network Namespace Support (aka NET_NS) is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via vectors involving IPv6 packets.	2009-04-22	7.1	CVE-2009-1360 CONFIRM CONFIRM
mark_girling -- myshoutpro	MyShoutPro 1.2 allows remote attackers to bypass authentication and gain administrative access by setting the admin_access cookie to 1.	2009-04-21	7.5	CVE-2008-6738 XF BID MILW0RM
mozilo -- mozilocms	Directory traversal vulnerability in index.php in moziloCMS 1.11 allows remote attackers to read arbitrary files via a .. (dot dot) in the page parameter. NOTE: this might be the same issue as CVE-2008-6126.2, which may have been fixed in 1.10.3.	2009-04-22	7.5	CVE-2009-1368 CONFIRM
neocrome -- seditio	SQL injection vulnerability in events/inc/events.inc.php in the Events plugin for Seditio CMS 1.0 allows remote attackers to execute arbitrary SQL commands via the c parameter to plug.php.	2009-04-24	7.5	CVE-2009-1411 XF VUPEN BID MILW0RM SECUNIA OSVDB
	Unspecified vulnerability in xtagent.exe			

novell -- netidentity_client1.2.3	in Novell NetIdentity Client before 1.2.4 allows remote attackers to execute arbitrary code by establishing an IPC$ connection to the XTIERRPCPIPE named pipe, and sending RPC messages that trigger a dereference of an arbitrary pointer.	2009-04-21	10.0	CVE-2009-1350 MISC VUPEN CONFIRM
opensolution -- quick.cms.lite	SQL injection vulnerability in index.php in Quick.Cms.Lite 0.5 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-04-24	7.5	CVE-2009-1410 XF BID MILW0RM
revou -- revou	Unrestricted file upload vulnerability in index.php in the Twitter Clone (TClone) plugin for ReVou Micro Blogging allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in settings/my_photo.	2009-04-24	7.5	CVE-2008-6751 XF BID MILW0RM SECUNIA
revou -- revou	adminlogin/password.php in the Twitter Clone (TClone) plugin for ReVou Micro Blogging does not verify the original password before changing passwords, which allows remote attackers to change the administrator's password and gain privileges via a direct request with modified newpass1 and newpass2 parameters in a Change operation.	2009-04-24	7.5	CVE-2008-6752 MILW0RM SECUNIA
shock-therapy -- rsmscript	RSMScript 1.21 allows remote attackers to bypass authentication and gain administrative privileges by setting the verified cookie to an arbitrary value and performing a direct request to (1) delete.php, (2) edit-submit.php, (3) edit.php, (4) submit.php, and (5) update.php, which bypasses the security check that is performed by verify.php.	2009-04-22	7.5	CVE-2008-6743 XF BID MILW0RM SECUNIA OSVDB
simple_machines -- simple_machines_forum	SQL injection vulnerability in Load.php in Simple Machines Forum (SMF) 1.1.4 and earlier allows remote attackers to execute arbitrary SQL commands by setting the db_character_set parameter to a multibyte character set such as big5, which causes the addslashes PHP function to produce a "\" (backslash) sequence that does not quote the "'" (single quote) character, as demonstrated via a manlabels action to index.php.	2009-04-21	7.5	CVE-2008-6741 XF BID MILW0RM
	Directory traversal vulnerability in			CVE-2009-1406

sweetphp -- totalcalendar	cms_detect.php in TotalCalendar 2.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the include parameter.	2009-04-24	7.5	1406 XF BID MILW0RM SECUNIA
symantec -- brightmail_gateway_appliance	Multiple unspecified vulnerabilities in the Control Center in Symantec Brightmail Gateway Appliance before 8.0.1 allow remote authenticated users to gain privileges, and possibly obtain sensitive information or hijack sessions of arbitrary users, via vectors involving (1) administrative scripts or (2) console functions.	2009-04-24	9.0	CVE-2009-0064 VUPEN CONFIRM SECTRACK
toddwoolums -- asp_download	Todd Woolums ASP Download management script 1.03 does not require authentication for setupdownload.asp, which allows remote attackers to gain administrator privileges via a direct request.	2009-04-21	7.5	CVE-2008-6739 XF MILW0RM
wireshark -- wireshark	Unspecified vulnerability in Wireshark before 1.0.7-0.1-1 has unknown impact and attack vectors.	2009-04-21	10.0	CVE-2009-1266 BUGTRAQ CONFIRM SECUNIA
xilisoft -- xilisoft_video_converter	Stack-based buffer overflow in ape_plugin.plg in Xilisoft Video Converter 3.1.53.0704n and 5.1.23.0402 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string in a .cue file.	2009-04-22	9.3	CVE-2009-1370 XF BID MILW0RM SECUNIA

Back to top

Medium Vulnerabilities (CVSS Score: 4.0 .. 6.9)

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
linux -- kernel	drivers/char/agp/generic.c in the agp subsystem in the Linux kernel before 2.6.30-rc3 does not zero out pages that may later be available to a user-space process, which allows local users to obtain sensitive information by reading these pages.	2009-04-24	4.9	CVE-2009-1192 CONFIRM BID CONFIRM
apache -- apache_http_server	mod_proxy_ajp.c in the mod_proxy_ajp module in the Apache HTTP Server 2.2.11 allows remote attackers to obtain sensitive response data, intended for a client that sent an earlier POST request with no request body, via an HTTP request.	2009-04-23	5.0	CVE-2009-1191 BID CONFIRM CONFIRM
	Integer overflow in the TIFF image decoding routines in CUPS 1.3.9 and earlier allows remote			

apple -- cups	attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via a crafted TIFF image, which is not properly handled by the (1) _cupsImageReadTIFF function in the imagetops filter and (2) imagetoraster filter, leading to a heap-based buffer overflow.	2009-04-23	6.8	CVE-2009-0163 CONFIRM
apple -- cups foolabs -- xpdf	Heap-based buffer overflow in Xpdf 3.02pl2 and earlier, CUPS 1.3.9, and probably other products, allows remote attackers to execute arbitrary code via a PDF file with crafted JBIG2 symbol dictionary segments.	2009-04-23	6.8	CVE-2009-0195 BUGTRAQ BUGTRAQ MISC MISC
apple -- cups	The web interface for CUPS before 1.3.10 does not validate the HTTP Host header in a client request, which makes it easier for remote attackers to conduct DNS rebinding attacks.	2009-04-24	6.4	CVE-2009-0164 CONFIRM CONFIRM
chcounter -- chcounter	SQL injection vulnerability in administration/index.php in chCounter 3.1.3 allows remote attackers to execute arbitrary SQL commands via the login_name parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-04-22	6.8	CVE-2009-1362 SECUNIA
china-on-site -- flexphpdirectory	Multiple SQL injection vulnerabilities in admin/usercheck.php in FlexPHPDirectory 0.0.1, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) checkuser and (2) checkpass parameters.	2009-04-24	6.8	CVE-2008-6749 XF MILW0RM SECUNIA OSVDB
circulargenius -- flat_calendar	Flat Calendar 1.1 does not properly restrict access to administrative functions, which allows remote attackers to (1) add new events via calAdd.php, as reachable from admin/add.php, or (2) delete events via admin/deleteEvent.php. NOTE: this is only a vulnerability when the administrator does not follow recommendations in the product's security documentation.	2009-04-21	6.4	CVE-2008-6736 XF BID BUGTRAQ OSVDB
clamav -- clamav	The CLI_ISCONTAINED macro in libclamav/others.h in ClamAV before 0.95.1 allows remote attackers to cause a denial of service (application crash) via a malformed file with UPack encoding.	2009-04-23	5.0	CVE-2009-1371 VUPEN BID
cybozu -- cybozu_dezie cybozu -- cybozu_garoon cybozu -- cybozu_office	Cross-site request forgery (CSRF) vulnerability in Cybozu Office 6, Cybozu Dezie before 6.0(1.0), and Cybozu Garoon 2.0.0 through 2.1.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2009-04-23	4.3	CVE-2008-6744 SECUNIA OSVDB JVNDB JVN CONFIRM CONFIRM

dotnetnuke -- dotnetnuke	Cross-site scripting (XSS) vulnerability in the Language skin object in DotNetNuke before 4.8.4 allows remote attackers to inject arbitrary web script or HTML via "newly generated paths."	2009-04-21	4.3	CVE-2008-6732 XF OSVDB CONFIRM SECUNIA
dotnetnuke -- dotnetnuke	Cross-site scripting (XSS) vulnerability in the error handling page in DotNetNuke 4.6.2 through 4.8.3 allows remote attackers to inject arbitrary web script or HTML via the querystring parameter.	2009-04-21	4.3	CVE-2008-6733 XF OSVDB CONFIRM SECUNIA
dotnetnuke -- dotnetnuke	Cross-site scripting (XSS) vulnerability in Website\admin\Sales\paypalipn.aspx in DotNetNuke (DNN) before 4.9.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to "name/value pairs" and "paypal IPN functionality."	2009-04-22	4.3	CVE-2009-1366 CONFIRM SECUNIA
dotproject -- dotproject	dotProject before 2.1.2 does not properly restrict access to administrative pages, which allows remote attackers to gain privileges. NOTE: some of these details are obtained from third party information.	2009-04-23	6.8	CVE-2008-6747 XF BID CONFIRM SECUNIA OSVDB
drupal -- print	Cross-site scripting (XSS) vulnerability in the Print (aka Printer, e-mail and PDF versions) module 5.x before 5.x-4.5 and 6.x before 6.x-1.5, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via content titles.	2009-04-20	4.3	CVE-2009-1343 VUPEN BID CONFIRM
e107 -- e107	SQL injection vulnerability in usersettings.php in e107 0.7.15 and earlier, when "Extended User Fields" is enabled and magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the hide parameter, a different vector than CVE-2005-4224 and CVE-2008-5320.	2009-04-24	5.1	CVE-2009-1409 XF BID MILW0RM SECUNIA OSVDB
foolabs -- xpdf	Multiple buffer overflows in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allow remote attackers to cause a denial of service (crash) via a crafted PDF file, related to (1) JBIG2SymbolDict::setBitmap and (2) JBIG2Stream::readSymbolDictSeg.	2009-04-23	4.3	CVE-2009-0146 REDHAT
foolabs -- xpdf	Multiple integer overflows in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allow remote attackers to cause a denial of service (crash) via a crafted PDF file, related to (1)	2009-04-23	4.3	CVE-2009-0147 REDHAT

	JBIG2Stream::readSymbolDictSeg, (2) JBIG2Stream::readSymbolDictSeg, and (3) JBIG2Stream::readGenericBitmap.			REDHAT
foolabs -- xpdf	The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, and other products allows remote attackers to cause a denial of service (crash) via a crafted PDF file that triggers a free of uninitialized memory.	2009-04-23	4.3	CVE-2009-0166 CONFIRM REDHAT SECUNIA
foolabs -- xpdf	The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to cause a denial of service (crash) via a crafted PDF file that triggers an out-of-bounds read.	2009-04-23	4.3	CVE-2009-0799 REDHAT
foolabs -- xpdf	Multiple "input validation flaws" in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allow remote attackers to execute arbitrary code via a crafted PDF file.	2009-04-23	6.8	CVE-2009-0800 CONFIRM REDHAT SECUNIA
foolabs -- xpdf	Integer overflow in the JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to execute arbitrary code via a crafted PDF file.	2009-04-23	6.8	CVE-2009-1179 REDHAT
foolabs -- xpdf	The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to execute arbitrary code via a crafted PDF file that triggers a free of invalid data.	2009-04-23	6.8	CVE-2009-1180 REDHAT
foolabs -- xpdf	The JBIG2 decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to cause a denial of service (crash) via a crafted PDF file that triggers a NULL pointer dereference.	2009-04-23	5.0	CVE-2009-1181 CONFIRM REDHAT SECUNIA
foolabs -- xpdf	The JBIG2 MMR decoder in Xpdf 3.02pl2 and earlier, CUPS 1.3.9 and earlier, Poppler before 0.10.6, and other products allows remote attackers to cause a denial of service (infinite loop and hang) via a crafted PDF file.	2009-04-23	4.3	CVE-2009-1183 REDHAT
gofoxy -- foxy	Foxy P2P software allows remote attackers to cause a denial of service (memory consumption) via a foxy URI with a download action and a large fs value.	2009-04-21	4.3	CVE-2008-6742 XF BID MILW0RM
homap -- homap	PHP remote file inclusion vulnerability in html/admin/modules/plugin_admin.php in HoMaP-CMS 0.1 allows remote attackers to execute arbitrary PHP code via a URL in the _settings[pluginpath] parameter.	2009-04-21	6.8	CVE-2008-6740 XF BID MILW0RM

horde -- turba_h3	Cross-site scripting (XSS) vulnerability in the contact display view in Turba Contact Manager H3 before 2.2.1 allows remote attackers to inject arbitrary web script or HTML via the contact name.	2009-04-23	4.3	CVE-2008-6746 XF BID SECUNIA MLIST CONFIRM
hp -- storage_essentials	Unspecified vulnerability in Secure NaviCLI in HP Storage Essentials 6.0.2 through 6.0.4 allows remote authenticated users to obtain "access" or "extended privileges" via unknown vectors.	2009-04-21	6.5	CVE-2009-0715 HP
hp -- storageworks_storage_mirroring	Unspecified vulnerability in HP StorageWorks Storage Mirroring 5 before 5.1.1.1090.15 allows remote attackers to cause a denial of service via unknown vectors.	2009-04-21	5.0	CVE-2009-0717 HP
linux -- kernel	fs/nfs/client.c in the Linux kernel before 2.6.23 does not properly initialize a certain structure member that stores the maximum NFS filename length, which allows local users to cause a denial of service (OOPS) via a long filename, related to the encode_lookup function.	2009-04-22	4.9	CVE-2009-1336 CONFIRM MLIST MLIST CONFIRM CONFIRM
linux -- kernel	The exit_notify function in kernel/exit.c in the Linux kernel before 2.6.30-rc1 does not restrict exit signals when the CAP_KILL capability is held, which allows local users to send an arbitrary signal to a process by running a program that modifies the exit_signal field and then uses an exec system call to launch a setuid application.	2009-04-22	4.4	CVE-2009-1337 CONFIRM CONFIRM
linux -- kernel	The kill_something_info function in kernel/signal.c in the Linux kernel before 2.6.28 does not consider PID namespaces when processing signals directed to PID -1, which allows local users to bypass the intended namespace isolation, and send arbitrary signals to all processes in all namespaces, via a kill command.	2009-04-22	4.6	CVE-2009-1338 CONFIRM CONFIRM MLIST CONFIRM
mahara -- mahara	Multiple cross-site scripting (XSS) vulnerabilities in Mahara 1.0.x before 1.0.11 and 1.1.x before 1.1.3 allow remote attackers to inject arbitrary web script or HTML via (1) the introduction field in a user profile or (2) an arbitrary text block in a user view.	2009-04-23	4.3	CVE-2009-0664 BID
mark_girling -- myshoutpro	Cross-site scripting (XSS) vulnerability in MyShoutPro before 1.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-04-21	4.3	CVE-2006-7238 CONFIRM
				CVE-2008-6748

megacubo -- megacubo	Eval injection vulnerability in Megacubo 5.0.7 allows remote attackers to inject and execute arbitrary PHP code via the play action in a mega:// URI.	2009-04-24	6.8	XF BID BUGTRAQ MILW0RM SECUNIA MISC OSVDB
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The browser engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to (1) nsAsyncInstantiateEvent::Run, (2) nsStyleContext::Destroy, (3) nsComputedDOMStyle::GetWidth, (4) the xslt_attributeset_ImportSameName.html test case for the XSLT stylesheet compiler, (5) nsXULDocument::SynchronizeBroadcastListener, (6) IsBindingAncestor, (7) PL_DHashTableOperate and nsEditor::EndUpdateViewBatch, and (8) gfxSkipCharsIterator::SetOffsets, and other vectors.	2009-04-22	5.0	CVE-2009-1302 CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The browser engine in Mozilla Firefox before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors related to nsSVGElement::BindToTree.	2009-04-22	5.0	CVE-2009-1303 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The JavaScript engine in Mozilla Firefox 3.x before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving (1) js_FindPropertyHelper, related to the definitions of Math and Date; and (2) js_CheckRedeclaration.	2009-04-22	5.0	CVE-2009-1304 CONFIRM CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The JavaScript engine in Mozilla Firefox before 3.0.9, Thunderbird before 2.0.0.22, and SeaMonkey before 1.1.16 allows remote attackers to cause a denial of service (application crash) and possibly trigger memory corruption via vectors involving JSOP_DEFVAR and properties that lack the JSPROP_PERMANENT attribute.	2009-04-22	5.0	CVE-2009-1305 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The jar: URI implementation in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey does not follow the Content-Disposition header of the inner URI, which allows remote attackers to conduct cross-site scripting (XSS) attacks and possibly other attacks via an uploaded .jar file	2009-04-22	4.3	CVE-2009-1306 CONFIRM CONFIRM

	with a "Content-Disposition: attachment" designation.			
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The view-source: URI implementation in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey does not properly implement the Same Origin Policy, which allows remote attackers to (1) bypass crossdomain.xml restrictions and connect to arbitrary web sites via a Flash file; (2) read, create, or modify Local Shared Objects via a Flash file; or (3) bypass unspecified restrictions and render content via vectors involving a jar: URI.	2009-04-22	6.8	CVE-2009-1307 CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Cross-site scripting (XSS) vulnerability in Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey allows remote attackers to inject arbitrary web script or HTML via vectors involving XBL JavaScript bindings and remote stylesheets, as exploited in the wild by a March 2009 eBay listing.	2009-04-22	4.3	CVE-2009-1308 CONFIRM MISC CONFIRM
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 3.0.9, Thunderbird, and SeaMonkey do not properly implement the Same Origin Policy for (1) XMLHttpRequest, involving a mismatch for a document's principal, and (2) XPCNativeWrapper.toString, involving an incorrect __proto__ scope, which allows remote attackers to conduct cross-site scripting (XSS) attacks and possibly other attacks via a crafted document.	2009-04-22	4.3	CVE-2009-1309 CONFIRM CONFIRM CONFIRM
mozilla -- firefox	Cross-site scripting (XSS) vulnerability in the MozSearch plugin implementation in Mozilla Firefox before 3.0.9 allows user-assisted remote attackers to inject arbitrary web script or HTML via a javascript: URI in the SearchForm element.	2009-04-22	4.3	CVE-2009-1310 CONFIRM
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.9 and SeaMonkey before 1.1.17 allow user-assisted remote attackers to obtain sensitive information via a web page with an embedded frame, which causes POST data from an outer page to be sent to the inner frame's URL during a SAVEMODE_FILEONLY save of the inner frame.	2009-04-22	4.3	CVE-2009-1311 CONFIRM CONFIRM
mozilla -- firefox mozilla -- seamonkey	Mozilla Firefox before 3.0.9 and SeaMonkey do not block javascript: URIs in Refresh headers in HTTP responses, which allows remote attackers to conduct cross-site scripting (XSS) attacks via vectors related to (1) injecting a Refresh header or (2) specifying the content of a Refresh header.	2009-04-22	4.3	CVE-2009-1312 CONFIRM
mozilo -- mozilocms	Cross-site scripting (XSS) vulnerability in index.php in moziloCMS 1.11 allows remote attackers to inject arbitrary web script or HTML via the query parameter in search action, a	2009-04-22	4.3	CVE-2009-1367 XF BID MILWORM

	different issue than CVE-2008-6127.2a.			MILW0RM CONFIRM
mozilo -- mozilocms	moziloCMS 1.11 allows remote attackers to obtain sensitive information via the (1) gal[] parameter to gallery.php, (2) page[] and (3) cat[] parameter to index.php, or (4) file[] parameter to download.php, which reveals the installation path in an error message.	2009-04-22	5.0	CVE-2009-1369 XF MILW0RM
pastel -- pastelcms	SQL injection vulnerability in admin.php in PastelCMS 0.8.0, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the user (Username) parameter.	2009-04-24	6.8	CVE-2009-1404 XF BID MILW0RM SECUNIA
pastel -- pastelcms	Directory traversal vulnerability in index.php in PastelCMS 0.8.0, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the set_lng parameter.	2009-04-24	6.8	CVE-2009-1405 XF BID MILW0RM SECUNIA
plone -- plonepas	The PlonePAS product 3.x before 3.9 and 3.2.x before 3.2.2, a product for Plone, does not properly handle the login form, which allows remote authenticated users to acquire the identity of an arbitrary user via unspecified vectors.	2009-04-23	6.0	CVE-2009-0662 CONFIRM
poppler -- poppler	Integer overflow in the JBIG2 decoding feature in Poppler before 0.10.6 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to CairoOutputDev (CairoOutputDev.cc).	2009-04-23	5.0	CVE-2009-1187 CONFIRM
poppler -- poppler	Integer overflow in the JBIG2 decoding feature in Poppler before 0.10.6 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to SplashBitmap (splash/SplashBitmap.cc).	2009-04-23	5.0	CVE-2009-1188 CONFIRM
redhat -- stronghold	Cross-site scripting (XSS) vulnerability in C2Net Stronghold 2.3 allows remote attackers to inject arbitrary web script or HTML via the URI.	2009-04-21	4.3	CVE-2009-1349 BID BUGTRAQ
rim -- blackberry_enterprise_server	Cross-site scripting (XSS) vulnerability in the "Customize Statistics Page" (admin/statistics/ConfigureStatistics) in the MDS Connection Service in Research in Motion (RIM) BlackBerry Enterprise Server (BES) before 4.1.6 MR5 allows remote attackers to inject arbitrary web script or HTML via the (1) customDate, (2) interval, (3) lastCustomInterval, (4) lastIntervalLength, (5) nextCustomInterval, (6) nextIntervalLength, (7) action, (8) delIntervalIndex, (9) addStatIndex, (10)	2009-04-22	4.3	CVE-2009-0307 BID CONFIRM SECUNIA

	delStatIndex, and (11) referenceTime parameters.			
sebastian_fernandez -- zervit	Buffer overflow in the http_parse_hex function in libz/misc.c in Zervit Webserver 0.02 allows remote attackers to cause a denial of service (daemon crash) via a long URI, related to http.c.	2009-04-21	5.0	CVE-2009-1353 CONFIRM CONFIRM BID BUGTRAQ MILW0RM
sergey_lyubka -- mongoose	Directory traversal vulnerability in Mongoose 2.4 allows remote attackers to read arbitrary files via a .. (dot dot) in the URI.	2009-04-21	4.0	CVE-2009-1354 XF BID BUGTRAQ MILW0RM
sun -- opensolaris	Unspecified vulnerability in the SCTP sockets implementation in Sun OpenSolaris snv_106 through snv_107 allows local users to cause a denial of service (panic) via unknown vectors.	2009-04-22	4.9	CVE-2009-1359 SUNALERT
sun -- java_system_delegated_administrator	CRLF injection vulnerability in da/DA/Login in Sun Java System Delegated Administrator 6.2 through 6.4 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the HELP_PAGE parameter.	2009-04-23	6.8	CVE-2009-1357 VUPEN SUNALERT CONFIRM SECTRACK
symantec -- brightmail_gateway_appliance	Cross-site scripting (XSS) vulnerability in the Control Center in Symantec Brightmail Gateway Appliance before 8.0.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2009-04-24	4.3	CVE-2009-0063 VUPEN CONFIRM SECTRACK
thaiquickcart -- thaiquickcart	Directory traversal vulnerability in qc/index.php in ThaiQuickCart 3 allows remote attackers to read arbitrary files via a .. (dot dot) in the sLanguage cookie.	2009-04-21	5.8	CVE-2008-6735 XF BID MILW0RM
tim_hockin -- acpid	The daemon in acpid before 1.0.10 allows remote attackers to cause a denial of service (CPU consumption and connectivity loss) by opening a large number of UNIX sockets without closing them, which triggers an infinite loop.	2009-04-24	5.0	CVE-2009-0798 CONFIRM
webspell -- webspell	Cross-site scripting (XSS) vulnerability in webSPELL 4.2.0c allows remote attackers to inject arbitrary web script or HTML allows remote attackers to inject arbitrary web script or HTML via Javascript events such as onmouseover in nested BBcode tags, as demonstrated using (1) email, (2) img, and (3) url tags.	2009-04-24	4.3	CVE-2009-1408 CONFIRM CONFIRM BID
wonko -- notftp	Directory traversal vulnerability in config.php in NotFTP 1.3.1 allows remote attackers to read	2009-04-	6.8	CVE-2009-1407 XF

wolfko -- flottp	arbitrary files via a .. (dot dot) in a certain languages[][file] parameter.	24	6.8	XF BID MILW0RM

Back to top

There were no low vulnerabilities recorded this week.