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**
	SQL injection vulnerability in articleCall.php in Bloginator 1A allows remote attackers to execute arbitrary SQL commands via the id parameter.	2009-03-24	7.5	CVE-2009-1049 XF BID MILW0RM MILW0RM SECUNIA
adobe -- acrobat adobe -- reader	Unspecified vulnerability in Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 might allow remote attackers to execute arbitrary code via unknown attack vectors related to JBIG2 and "input validation," a different vulnerability than CVE-2009-1061 and CVE-2009-1062.	2009-03-24	9.3	CVE-2009-0193 CONFIRM
adobe -- acrobat_professional adobe -- acrobat_reader	Heap-based buffer overflow in Adobe Acrobat Reader and Acrobat Professional 7.1.0, 8.1.3, 9.0.0, and other versions allows remote attackers to execute arbitrary code via a PDF file containing a JBIG2 stream with a size inconsistency related to an unspecified table.	2009-03-24	7.5	CVE-2009-0928 CONFIRM IDEFENSE

adobe -- acrobat adobe -- reader	Unspecified vulnerability in Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 might allow remote attackers to execute arbitrary code via unknown attack vectors related to JBIG2 and "input validation," a different vulnerability than CVE-2009-0193 and CVE-2009-1062.	2009-03-24	9.3	CVE-2009-1061 CONFIRM
apple -- safari	Unspecified vulnerability in Apple Safari on Mac OS X 10.5.6 allows remote attackers to execute arbitrary code via unknown vectors triggered by clicking on a link, as demonstrated by Charlie Miller during a PWN2OWN competition at CanSecWest 2009.	2009-03-24	9.3	CVE-2009-1060 MISC MISC MISC MISC
argyllcms -- cms ghostscript -- ghostscript	icc.c in the International Color Consortium (ICC) Format library (aka icclib), as used in Ghostscript 8.64 and earlier and Argyll Color Management System (CMS) 1.0.3 and earlier, allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code by using a device file for processing a crafted image file associated with large integer values for certain sizes, related to an ICC profile in a (1) PostScript or (2) PDF file with embedded images.	2009-03-23	9.3	CVE-2009-0584 AUSCERT FEDORA FEDORA CONFIRM CONFIRM XF VUPEN VUPEN VUPEN UBUNTU BID BUGTRAQ REDHAT GENTOO DEBIAN CONFIRM CONFIRM SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA CONFIRM
bosdev -- bos_classifieds	SQL injection vulnerability in index.php in BosDev BosClassifieds allows remote attackers to execute arbitrary SQL commands via the cat_id parameter, a different vector than CVE-2008-1838.	2009-03-25	7.5	CVE-2008-6526 XF BID MILW0RM
				CVE-2009-1068

bsplayer -- bs.player	Stack-based buffer overflow in BS.Player (bsplayer) 2.32 Build 975 Free and 2.34 Build 980 PRO and earlier allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a long hostname in a .bsl playlist file.	2009-03-26	9.3	1008 XF BID BUGTRAQ MILW0RM MILW0RM SECUNIA MISC
cale_dunlap -- openinvoice	auth.php in openInvoice 0.90 beta and earlier allows remote attackers to bypass authentication and gain privileges by setting the oiauth cookie. NOTE: this can be leveraged with a separate vulnerability in resetpass.php to modify passwords for arbitrary users.	2009-03-25	7.5	CVE-2008-6523 XF BID MILW0RM
cisco -- ios	Unspecified vulnerability in Cisco IOS 12.0 through 12.4, when configured with (1) IP Service Level Agreements (SLAs) Responder, (2) Session Initiation Protocol (SIP), (3) H.323 Annex E Call Signaling Transport, or (4) Media Gateway Control Protocol (MGCP) allows remote attackers to cause a denial of service (blocked input queue on the inbound interface) via a crafted UDP packet.	2009-03-27	7.8	CVE-2009-0631 CONFIRM CISCO
cisco -- ios	The SSLVPN feature in Cisco IOS 12.3 through 12.4 allows remote attackers to cause a denial of service (device reload or hang) via a crafted HTTPS packet.	2009-03-27	7.8	CVE-2009-0626 XF VUPEN BID CONFIRM CISCO SECTRACK SECUNIA
cisco -- cisco_ios	Memory leak in the SSLVPN feature in Cisco IOS 12.3 through 12.4 allows remote attackers to cause a denial of service (memory consumption and device crash) by disconnecting an SSL session in an abnormal manner, leading to a Transmission Control Block (TCB) leak.	2009-03-27	9.0	CVE-2009-0628 XF VUPEN BID CONFIRM CISCO SECTRACK SECUNIA
	The (1) Cisco Unified Communications Manager Express; (2) SIP Gateway Signaling Support Over Transport Layer Security (TLS) Transport; (3) Secure Signaling and Media			CVE-2009

cisco -- ios	Encryption; (4) Blocks Extensible Exchange Protocol (BEEP); (5) Network Admission Control HTTP Authentication Proxy; (6) Per-user URL Redirect for EAPoUDP, Dot1x, and MAC Authentication Bypass; (7) Distributed Director with HTTP Redirects; and (8) TCP DNS features in Cisco IOS 12.0 through 12.4 do not properly handle IP sockets, which allows remote attackers to cause a denial of service (outage or resource consumption) via a series of crafted TCP packets.	2009-03-27	7.1	CVE-2009-0630 XF VUPEN BID CISCO CONFIRM SECTRACK SECUNIA
cisco -- cisco_ios	Multiple unspecified vulnerabilities in the (1) Mobile IP NAT Traversal feature and (2) Mobile IPv6 subsystem in Cisco IOS 12.3 through 12.4 allow remote attackers to cause a denial of service (input queue wedge and interface outage) via MIPv6 packets, aka Bug ID CSCsm97220.	2009-03-27	7.1	CVE-2009-0633 XF VUPEN BID CONFIRM CISCO SECTRACK SECUNIA
cisco -- cisco_ios	Multiple unspecified vulnerabilities in the home agent (HA) implementation in the (1) Mobile IP NAT Traversal feature and (2) Mobile IPv6 subsystem in Cisco IOS 12.3 through 12.4 allow remote attackers to cause a denial of service (input queue wedge and interface outage) via an ICMP packet, aka Bug ID CSCso05337.	2009-03-27	7.1	CVE-2009-0634 XF VUPEN BID CONFIRM CISCO SECTRACK SECUNIA
citadel -- webcit	Format string vulnerability in the mini_calendar component in Citadel.org WebCit 7.22, and other versions before 7.39, allows remote attackers to execute arbitrary code via unspecified vectors.	2009-03-26	7.5	CVE-2009-0364 BID
deluxebb -- deluxebb	SQL injection vulnerability in misc.php in DeluxeBB 1.3 and earlier allows remote attackers to execute arbitrary SQL commands via the qorder parameter, a different vector than CVE-2005-2989 and CVE-2006-2503.	2009-03-20	7.5	CVE-2009-1033 XF BID MILW0RM SECUNIA
freebsd -- freebsd	The ktimer feature (sys/kern/kern_time.c) in FreeBSD 7.0, 7.1, and 7.2 allows local users to overwrite arbitrary kernel memory via an out-of-bounds timer value.	2009-03-26	7.2	CVE-2009-1041 XF BID MILW0RM FREEBSD

getpixie -- pixie	SQL injection vulnerability in index.php in Pixie CMS 1.01a allows remote attackers to execute arbitrary SQL commands via the x parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-26	7.5	CVE-2009-1065 XF SECUNIA OSVDB
getpixie -- pixie_cms	SQL injection vulnerability in the referral function in admin/lib/lib_logs.php in Pixie CMS 1.01a allows remote attackers to execute arbitrary SQL commands via the Referer HTTP header in a request.	2009-03-26	7.5	CVE-2009-1066 XF BID MILW0RM SECUNIA OSVDB MISC FULLDISC
gimp -- gimp littlecms -- lcms mozilla -- firefox sun -- openjdk	Multiple integer overflows in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allow context-dependent attackers to execute arbitrary code via a crafted image file that triggers a heap-based buffer overflow. NOTE: some of these details are obtained from third party information.	2009-03-23	9.3	CVE-2009-0723 BID
gimp -- gimp littlecms -- lcms mozilla -- firefox sun -- openjdk	Multiple stack-based buffer overflows in the ReadSetOfCurves function in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allow context-dependent attackers to execute arbitrary code via a crafted image file associated with a large integer value for the (1) input or (2) output channel, related to the ReadLUT_A2B and ReadLUT_B2A functions.	2009-03-23	9.3	CVE-2009-0733 CONFIRM XF VUPEN UBUNTU BID BUGTRAQ REDHAT MISC DEBIAN SECUNIA SECUNIA SECUNIA MISC MISC
go4i -- go41.net_asp_forum	SQL injection vulnerability in forum.asp in GO4I.NET ASP Forum 1.0 allows remote attackers to execute arbitrary SQL commands via the iFor parameter.	2009-03-25	7.5	CVE-2008-6527 XF BID MILW0RM
	Stack-based buffer overflow in			CVE-2009-0920 XF

hp -- network_node_manager	OvCgi/Toolbar.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to execute arbitrary code via a long OvOSLocale cookie, a variant of CVE-2008-0067.	2009-03-24	7.5	XF VUPEN SECTRACK BUGTRAQ MISC SECUNIA HP HP
hp -- network_node_manager	Multiple heap-based buffer overflows in OvCgi/Toolbar.exe in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allow remote attackers to execute arbitrary code via (1) a long OvAcceptLang cookie, which triggers the error in ov.dll and ovwww.dll, or (2) a long Accept-Language HTTP header, which triggers the error in ovwww.dll or libovwww.so.4.	2009-03-24	7.5	CVE-2009-0921 XF VUPEN SECTRACK BID BID BUGTRAQ MISC SECUNIA HP HP
ibm -- access_support_activex_control	Stack-based buffer overflow in the GetXMLValue method in the IBM Access Support ActiveX control in IbmEgath.dll, as distributed on IBM and Lenovo computers, allows remote attackers to execute arbitrary code via unspecified vectors.	2009-03-25	9.3	CVE-2009-0215 CERT-VN VUPEN BID
ichitaro -- ichitaro ichitaro -- ichitaro_viewer	Unspecified vulnerability in JustSystems Ichitaro 13, 2004 through 2008, Lite2, and Ichitaro viewer 5.1.5.0 and earlier allows remote attackers to execute arbitrary code via a crafted file, as exploited in the wild by Trojan.Tarodrop.H in March 2009.	2009-03-24	9.3	CVE-2009-1054 CONFIRM
igniterealtime -- openfire	Directory traversal vulnerability in the AuthCheck filter in the Admin Console in Openfire 3.6.0a and earlier allows remote attackers to bypass authentication and access the admin interface via a .. (dot dot) in a URI that matches the Exclude-Strings list, as demonstrated by a /setup/setup-/.. sequence in a URI.	2009-03-23	7.5	CVE-2008-6508 CONFIRM CONFIRM
igniterealtime -- openfire	SQL injection vulnerability in CallLogDAO in SIP Plugin in Openfire 3.6.0a and earlier allows remote attackers to execute arbitrary SQL commands via the type parameter to	2009-03-23	7.5	CVE-2008-6509 XF VUPEN BID BUGTRAQ MILW0RM

	sipark-log-summary.jsp.			CONFIRM MISC MISC OSVDB
imatix -- xitami	Format string vulnerability in Xitami Web Server 2.2a through 2.5c2, and possibly other versions, allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via format string specifiers in a Long Running Web Process (LRWP) request, which triggers incorrect logging code involving the sendfmt function in the SMT kernel.	2009-03-25	10.0	CVE-2008-6519 XF BID MILW0RM MISC
imatix -- xitami	Multiple format string vulnerabilities in the SSI filter in Xitami Web Server 2.5c2, and possibly other versions, allow remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via format string specifiers in a URI that ends in (1) .ssi, (2) .shtm, or (3) .shtml, which triggers incorrect logging code involving the sendfmt function in the SMT kernel.	2009-03-25	10.0	CVE-2008-6520 XF BID MISC
kamads -- bloginator	Bloginator 1A allows remote attackers to bypass authentication and gain administrative access by setting the identifyYourself cookie.	2009-03-24	7.5	CVE-2009-1050 XF BID MILW0RM SECUNIA
microsmarts -- zipitfast!	MicroSmarts Enterprise ZipItFast! 3.0 allows remote attackers to execute arbitrary code via a crafted .zip file that triggers memory corruption, related to a "format string buffer overflow." NOTE: CVE has not investigated whether the specified file.zip file can be used for exploitation of this product.	2009-03-24	10.0	CVE-2009-1057 MILW0RM SECUNIA OSVDB
mozilla -- firefox	Unspecified vulnerability in Mozilla Firefox 3.0.7 on Windows 7 allows remote attackers to execute arbitrary code via unknown vectors triggered by clicking on a link, as demonstrated by Nils during a PWN2OWN competition at CanSecWest 2009.	2009-03-23	9.3	CVE-2009-1044 BID MISC MISC MISC MISC MISC MISC MISC MISC

mozilla -- firefox	The txMozillaXSLTProcessor::TransformToDoc function in Mozilla Firefox 3.0.7 and earlier allows remote attackers to cause a denial of service (crash) via an XML file with a crafted XSLT transform.	2009-03-26	9.3	CVE-2009-1169 CONFIRM MILW0RM MISC
newshowler -- 1.0.3_beta	SQL injection vulnerability in NewsHOWLER 1.03 Beta allows remote attackers to execute arbitrary SQL commands via the news_user cookie parameter.	2009-03-25	7.5	CVE-2008-6517 XF BID BUGTRAQ OSVDB
nice -- nicephpscripts	SQL injection vulnerability in the Admin Panel in Nice PHP FAQ Script (Knowledge base Script) allows remote attackers to execute arbitrary SQL commands via the Password parameter (aka the pass field).	2009-03-25	7.5	CVE-2008-6525 XF BID MILW0RM
paypalestores -- paypal_estores	admin/settings.php in PayPal eStores allows remote attackers to bypass intended access restrictions and change the administrative password via a direct request with a modified NewAdmin parameter.	2009-03-26	7.5	CVE-2008-6535 XF MILW0RM SECUNIA OSVDB
phpmyadmin -- phpmyadmin	CRLF injection vulnerability in bs_disp_as_mime_type.php in the BLOB streaming feature in phpMyAdmin before 3.1.3.1 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the (1) c_type and possibly (2) file_type parameters.	2009-03-26	7.5	CVE-2009-1149 CONFIRM MISC
phpmyadmin -- phpmyadmin	Static code injection vulnerability in setup.php in phpMyAdmin 2.11.x before 2.11.9.5 and 3.x before 3.1.3.1 allows remote attackers to inject arbitrary PHP code into a configuration file via the save action.	2009-03-26	7.5	CVE-2009-1151 CONFIRM
powerzip -- powerzip	Stack-based buffer overflow in Trident PowerZip 7.2 might allow remote attackers to execute arbitrary code via a crafted .zip file. NOTE: CVE has not investigated whether the specified file.zip file can be used for exploitation of this product.	2009-03-24	9.3	CVE-2009-1059 MILW0RM
pplive -- pplive	Multiple argument injection vulnerabilities in PPLive.exe in PPLive 1.9.21 and earlier allow remote attackers to execute arbitrary code via a UNC share pathname in the LoadModule argument to the (1) synacast, (2)	2009-03-25	9.3	CVE-2009-1087 XF VUPEN

	Play, (3) pplsv, or (4) ppvod URI handler. NOTE: some of these details are obtained from third party information.			MILW0RM SECUNIA
randomsoftware -- icarus	Stack-based buffer overflow in Icarus 2.0 allows remote attackers to cause a denial of service (application crach) or execute arbitrary code via a crafted Portable Game Notation (.pgn) file.	2009-03-26	9.3	CVE-2009-1071 XF BID MILW0RM SECUNIA OSVDB
siemens -- gigaset_se461__wimax_router	Siemens Gigaset SE461 WiMAX router 1.5-BL024.9.6401, and possibly other versions, allows remote attackers to cause a denial of service (device restart and loss of configuration) by connecting to TCP port 53, then closing the connection.	2009-03-26	7.3	CVE-2009-1152 XF BID MILW0RM MISC
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 allows remote authenticated users to gain privileges by submitting crafted commands to the Admin Console, as demonstrated by privileges for account creation and other administrative capabilities, related to the saveNoValidate action and saveNoValidateAllowedFormsAndWorkflows IDs.	2009-03-25	9.0	CVE-2009-1082 BID CONFIRM CONFIRM CONFIRM
sun -- jdk sun -- jre	Unspecified vulnerability in the LDAP implementation in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier; 6 Update 12 and earlier; SDK and JRE 1.3.1_24 and earlier; and 1.4.2_19 and earlier allows remote LDAP servers to execute arbitrary code via unknown vectors related to serialized data.	2009-03-25	10.0	CVE-2009-1094 SUNALERT MISC
sun -- jdk sun -- jre	Integer overflow in unpack200 in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier, and 6 Update 12 and earlier, allows remote attackers to access files or execute arbitrary code via a JAR file with crafted Pack200 headers.	2009-03-25	7.5	CVE-2009-1095 SUNALERT MISC
sun -- jdk sun -- jre	Buffer overflow in unpack200 in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier, and 6 Update 12 and earlier, allows remote attackers to access files or execute arbitrary code via a JAR file with crafted Pack200	2009-03-25	10.0	CVE-2009-1096 SUNALERT MISC

	headers.			
sun -- jdk sun -- jre	Multiple buffer overflows in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12 and earlier allow remote attackers to access files or execute arbitrary code via a crafted (1) PNG image, aka CR 6804996, and (2) GIF image, aka CR 6804997.	2009-03-25	7.5	CVE-2009-1097 SUNALERT
sun -- jdk sun -- jre	Buffer overflow in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier; 6 Update 12 and earlier; 1.4.2_19 and earlier; and 1.3.1_24 and earlier allows remote attackers to access files or execute arbitrary code via a crafted GIF image, aka CR 6804998.	2009-03-25	10.0	CVE-2009-1098 SUNALERT
sun -- java	Integer signedness error in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier, and 6 Update 12 and earlier, allows remote attackers to access files or execute arbitrary code via a crafted Type1 font, which triggers a buffer overflow.	2009-03-25	7.5	CVE-2009-1099 SUNALERT MISC
sun -- java	The Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12, 11, and 10 allows user-assisted remote attackers to cause a trusted applet to run in an older JRE version, which can be used to exploit vulnerabilities in that older version, aka CR 6706490.	2009-03-25	7.5	CVE-2009-1105 SUNALERT
vwsolutions -- null_ftp	Incomplete blacklist vulnerability in NULL FTP Server Free and Pro 1.1.0.7 allows remote authenticated users to execute arbitrary commands via a custom SITE command containing shell metacharacters such as "&" (ampersand) in the middle of an argument.	2009-03-26	7.1	CVE-2008-6534 XF CONFIRM VUPEN BID OSVDB MILW0RM MISC SECUNIA
winasm -- winasm_studio	Buffer overflow in WinAsm Studio 5.1.5.0 allows user-assisted remote attackers to execute arbitrary code via a crafted project (.wap) file.	2009-03-20	9.3	CVE-2009-1040 XF BID MILW0RM SECUNIA OSVDB
				CVE-2009

yabsoft -- advanced_image_hosting_script	SQL injection vulnerability in gallery_list.php in YABSoft Advanced Image Hosting (AIH) Script 2.3 allows remote attackers to execute arbitrary SQL commands via the gal parameter.	2009-03-20	7.5	CVE-2009-1032 XF BID MILW0RM SECUNIA
zipgenius -- zipgenius	Stack-based buffer overflow in ZipGenius might allow remote attackers to execute arbitrary code via a crafted .zip file that triggers an SEH overwrite. NOTE: it is possible that this overlaps CVE-2005-3317. NOTE: CVE has not investigated whether the specified file.zip file can be used for exploitation of this product.	2009-03-24	10.0	CVE-2009-1058 MILW0RM

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
adobe -- acrobat_reader	Unspecified vulnerability in Adobe Acrobat Reader 9 before 9.1, 8 before 8.1.4, and 7 before 7.1.1 might allow remote attackers to execute arbitrary code via unknown attack vectors related to JBIG2 and "input validation," a different vulnerability than CVE-2009-0193 and CVE-2009-1061.	2009-03-24	6.4	CVE-2009-1062 CONFIRM
aphpkb -- aphpkb	Unrestricted file upload vulnerability in saa.php in Andy's PHP Knowledgebase (aphpkb) 0.92.9 allows remote attackers to execute arbitrary code by uploading a file with an executable extension, then accessing it via a link that is listed by authors.php.	2009-03-24	6.8	CVE-2008-6513 CONFIRM
argyllcms -- cms ghostscript -- ghostscript	Multiple integer overflows in icc.c in the International Color Consortium (ICC) Format library (aka icclib), as used in Ghostscript 8.64 and earlier and Argyll Color Management System (CMS) 1.0.3 and earlier, allow context-dependent attackers to cause a denial of service (heap-based buffer overflow and	2009-03-23	6.8	CVE-2009-0583 AUSCERT FEDORA FEDORA CONFIRM CONFIRM XF VUPEN VUPEN VUPEN UBUNTU BID BUGTRAQ

ghostscript -- ghostscript	application crash) or possibly execute arbitrary code by using a device file for a translation request that operates on a crafted image file and targets a certain "native color space," related to an ICC profile in a (1) PostScript or (2) PDF file with embedded images.	25		BUGTRAQ REDHAT GENTOO DEBIAN CONFIRM CONFIRM SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA CONFIRM
atlassian -- jira	The WebWork 1 web application framework in Atlassian JIRA before 3.13.2 allows remote attackers to invoke exposed public JIRA methods via a crafted URL that is dynamically transformed into method calls, aka "WebWork 1 Parameter Injection Hole."	2009-03-26	6.8	CVE-2008-6531 CONFIRM
brother_soft -- exescope	Buffer overflow in eXeScope 6.50 allows user-assisted remote attackers to execute arbitrary code via a crafted executable (.exe) file.	2009-03-26	6.8	CVE-2009-1063 BID MILW0RM
cale_dunlap -- openinvoice	resetpass.php in openInvoice 0.90 beta and earlier allows remote authenticated users to change the passwords of arbitrary users via a modified uid parameter. NOTE: this can be leveraged with a separate vulnerability in auth.php to modify passwords without authentication.	2009-03-25	6.5	CVE-2008-6524 XF BID MILW0RM
chaozz -- fubarforum	FubarForum 1.6 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing user credentials via a direct request for user.tsv.	2009-03-24	5.0	CVE-2009-1051 BUGTRAQ MISC
chaozz -- fireant	FireAnt 1.3 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing user credentials via a direct request for user.tsv.	2009-03-24	5.0	CVE-2009-1052 BUGTRAQ MISC
chaozz -- chaozzdb	chaozzDB 1.2 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database	2009-03-24	5.0	CVE-2009-1053 BUGTRAQ

	containing user credentials via a direct request for user.tsv.			MISC
cisco -- ios cisco -- ios_s cisco -- ios_t cisco -- ios_xr cisco -- ios	The (1) Airline Product Set (aka ALPS), (2) Serial Tunnel Code (aka STUN), (3) Block Serial Tunnel Code (aka BSTUN), (4) Native Client Interface Architecture (NCIA) support, (5) Data-link switching (aka DLSw), (6) Remote Source-Route Bridging (RSRB), (7) Point to Point Tunneling Protocol (PPTP), (8) X.25 for Record Boundary Preservation (RBP), (9) X.25 over TCP (XOT), and (10) X.25 Routing features in Cisco IOS 12.2 and 12.4 allows remote attackers to cause a denial of service (device reload) via a series of crafted TCP packets.	2009-03-27	5.4	CVE-2009-0629 XF VUPEN BID CISCO CONFIRM SECTRACK SECUNIA
compiz -- compiz_fusion	The Expo plugin in Compiz Fusion 0.7.8 allows local users with physical access to drag the screen saver aside and access the locked desktop by using Expo mouse shortcuts, a related issue to CVE-2007-3920.	2009-03-24	6.2	CVE-2008-6514 BID
devraj_mukherjee -- openterracotta	index.php in Terracotta (aka OpenTerracotta) 0.6.1 allows remote attackers to obtain sensitive information via an invalid File parameter, which reveals the installation path in an error message.	2009-03-25	5.0	CVE-2008-6521 XF BUGTRAQ
devraj_mukherjee -- openterracotta	Multiple directory traversal vulnerabilities in the RenderFile function in ContentRender.class.php in Terracotta (aka OpenTerracotta) 0.6.1, and possibly other versions, allow remote attackers to list arbitrary directories and read arbitrary files via a .. (dot dot) in the (1) CurrentDirectory and (2) File parameters to index.php.	2009-03-25	6.8	CVE-2008-6522 XF BID BUGTRAQ
drupal -- plus1	Cross-site request forgery (CSRF) vulnerability in the Plus 1 module before 6.x-2.6, a module for Drupal, allows remote attackers to cast votes for content via unspecified aspects of the URI.	2009-03-20	6.8	CVE-2009-1036 CONFIRM
drupal -- print	Unspecified vulnerability in the Send by e-mail module in the "Printer, e-mail and PDF versions" module 5.x before 5.x-4.4 and 6.x before 6.x-1.4, a module for	2009-03-20	5.0	CVE-2009-1037

	Drupal, allows remote attackers to send unlimited spam messages via unknown vectors related to the flood control API.	20		CONFIRM
drupal -- drupal drupal -- print	Cross-site scripting (XSS) vulnerability in the Send by e-mail module in the "Printer, e-mail and PDF versions" module 5.x before 5.x-4.4 and 6.x before 6.x-1.4, a module for Drupal, allows remote attackers to inject arbitrary web script or HTML via vectors involving outbound HTML e-mail.	2009-03-23	4.3	CVE-2009-1047 CONFIRM
drupal -- content_construction_kit	Multiple cross-site scripting (XSS) vulnerabilities in the node edit form feature in Drupal Content Construction Kit (CCK) 6.x before 6.x-2.2, a module for Drupal, allow remote attackers to inject arbitrary web script or HTML via the (1) titles of candidate referenced nodes in the Node reference sub-module and the (2) names of candidate referenced users in the User reference sub-module.	2009-03-26	4.3	CVE-2009-1069 XF BID SECUNIA OSVDB OSVDB
drupal -- drupal	Multiple cross-site request forgery (CSRF) vulnerabilities in the update feature in Drupal 5.x before 5.13 and 6.x before 6.7 allow remote attackers to perform unauthorized actions as the superuser via unspecified vectors, as demonstrated by causing the superuser to "execute old updates" that modify the database.	2009-03-26	6.8	CVE-2008-6532 CONFIRM
drupal -- drupal	Drupal 5.x before 5.13 and 6.x before 6.7 does not delete all related content when an input format is deleted, which prevents the content from being properly filtered and allows remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.	2009-03-26	4.3	CVE-2008-6533 CONFIRM
expressionengine -- expressionengine	Cross-site scripting (XSS) vulnerability in system/index.php in ExpressionEngine 1.6.4 through 1.6.6, and possibly earlier versions, allows remote attackers to inject arbitrary web script or HTML via the avatar parameter.	2009-03-26	4.3	CVE-2009-1070 XF BID BUGTRAQ MISC SECUNIA CONFIRM
	Cross-site scripting (XSS) vulnerability in			CVE-2008-

ezonescripts -- living_local	listtest.php in eZoneScripts Living Local 1.1 allows remote attackers to inject arbitrary web script or HTML via the r parameter.	2009-03-26	4.3	6529 XF BID MILW0RM
ezonescripts -- living_local	Unrestricted file upload vulnerability in editimage.php in eZoneScripts Living Local 1.1 allows remote authenticated administrators to execute arbitrary PHP code by uploading a file with an executable extension, then accessing it via a direct request to the uploaded file.	2009-03-26	6.0	CVE-2008-6530 XF BID MILW0RM
geovision -- liveaudio_activex_control	Use after free vulnerability in the LIVEAUDIO.LiveAudioCtrl.1 ActiveX control in LIVEAU~1.OCX 7.0 for GeoVision DVR systems allows remote attackers to execute arbitrary code by calling the GetAudioPlayingTime method with certain arguments.	2009-03-25	6.8	CVE-2009-1092 XF BID BUGTRAQ MILW0RM MISC
getpixie -- pixie_cms	Cross-site scripting (XSS) vulnerability in index.php in Pixie CMS 1.01a allows remote attackers to inject arbitrary web script or HTML via the x parameter.	2009-03-26	5.0	CVE-2009-1067 XF BID MILW0RM SECUNIA OSVDB MISC FULLDISC
gimp -- gimp littlecms -- lcms mozilla -- firefox sun -- openjdk	Memory leak in LittleCMS (aka lcms or liblcms) before 1.18beta2, as used in Firefox 3.1beta, OpenJDK, and GIMP, allows context-dependent attackers to cause a denial of service (memory consumption and application crash) via a crafted image file.	2009-03-23	4.3	CVE-2009-0581 VUPEN BID
google -- gears	Cross-domain vulnerability in the WorkerPool API in Google Gears before 0.5.4.2 allows remote attackers to bypass the Same Origin Policy and the intended access restrictions of the allowCrossOrigin function by hosting an assumed-safe file type containing Google Gear commands on the target domain, then accessing that file from the attacking domain, whose response headers are not checked and cause the worker code to run in the target domain.	2009-03-24	4.3	CVE-2008-6512 XF BID SECUNIA CONFIRM MISC

hannonhill -- cascade	Hannon Hill Cascade Server 5.7 and other versions allows remote authenticated users to execute arbitrary programs or Java code via a crafted XSLT stylesheet with "extension elements and extension functions" that trigger code execution by Xalan-Java, as demonstrated using xalan://java.lang.Runtime.	2009-03-25	5.5	CVE-2009-1088 XF BID BUGTRAQ MILW0RM
hp -- hp-ux	Unspecified vulnerability in HP-UX B.11.11 running VERITAS Oracle Disk Manager (VRTSodm) 3.5, B.11.23 running VRTSodm 4.1 or VERITAS File System (VRTSvxfs) 4.1, B.11.23 running VRTSodm 5.0 or VRTSvxfs 5.0, and B.11.31 running VRTSodm 5.0 allows local users to gain root privileges via unknown vectors.	2009-03-24	6.8	CVE-2009-0207 BID HP HP
ibm -- rational_appscan	IBM Rational AppScan Enterprise before 5.5 FP1 allows remote attackers to read arbitrary exported reports by "forcefully browsing."	2009-03-24	5.0	CVE-2009-1056 BID AIXAPAR SECUNIA
ibm -- websphere_application_server	The Web Services Security component in IBM WebSphere Application Server 7.0 before Fix Pack 1 (7.0.0.1), 6.1 before Fix Pack 23 (6.1.0.23),and 6.0.2 before Fix Pack 33 (6.0.2.33) does not properly enforce (1) nonce and (2) timestamp expiration values in WS-Security bindings as stored in the com.ibm.wsspi.wssecurity.core custom property, which allows remote authenticated users to conduct session hijacking attacks.	2009-03-24	5.5	CVE-2009-0891 CONFIRM CONFIRM CONFIRM
igniterealtime -- openfire	Cross-site scripting (XSS) vulnerability in login.jsp in the Admin Console in Openfire 3.6.0a and earlier allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2009-03-23	4.3	CVE-2008-6510 XF VUPEN BID BUGTRAQ MILW0RM CONFIRM MISC
igniterealtime -- openfire	Open redirect vulnerability in login.jsp in Openfire 3.6.0a and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via the	2009-03-23	5.8	CVE-2008-6511 BUGTRAQ MILW0RM

	url parameter.			MISC
kernel -- linux	The ecryptfs_write_metadata_to_contents function in the eCryptfs functionality in the Linux kernel 2.6.28 before 2.6.28.9 uses an incorrect size when writing kernel memory to an eCryptfs file header, which triggers an out-of-bounds read and allows local users to obtain portions of kernel memory.	2009-03-24	4.9	CVE-2009-0787 BID
linux -- kernel	nfsd in the Linux kernel before 2.6.28.9 does not drop the CAP_MKNOD capability before handling a user request in a thread, which allows local users to create device nodes, as demonstrated on a filesystem that has been exported with the root_squash option.	2009-03-24	4.9	CVE-2009-1072 XF VUPEN CONFIRM MLIST SECUNIA SECUNIA CONFIRM
nlnetlabs -- ldns	Heap-based buffer overflow in the ldns_rr_new_frm_str_internal function in ldns 1.4.x allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via a DNS resource record (RR) with a long (1) class field (clas variable) and possibly (2) TTL field.	2009-03-25	6.4	CVE-2009-1086 MLIST MISC
openssl -- openssl	The ASN1_STRING_print_ex function in OpenSSL before 0.9.8k allows remote attackers to cause a denial of service (invalid memory access and application crash) via vectors that trigger printing of a (1) BMPString or (2) UniversalString with an invalid encoded length.	2009-03-27	5.0	CVE-2009-0590 VUPEN BID CONFIRM
orbit_downloader -- orbit_downloader orbitdownloader -- orbit_downloader	Argument injection vulnerability in orbitmxt.dll 2.1.0.2 in the Orbit Downloader 2.8.7 and earlier ActiveX control allows remote attackers to overwrite arbitrary files via whitespace and a command-line switch, followed by a full pathname, in the third argument to the download method.	2009-03-26	6.4	CVE-2009-1064 XF MISC BID MILW0RM
phpbb -- phpbb	Unspecified vulnerability in phpBB before 3.0.4 allows attackers to obtain sensitive information via unknown vectors related to the lack of password prompts for a private message that quotes a post in a	2009-03-23	5.0	CVE-2008-6507 CONFIRM CONFIRM OSVDB MLIST

	password-protected forum.			MLIST SECUNIA
phpkf -- phpkf-portal	Multiple directory traversal vulnerabilities in phpKF-Portal 1.10 allow remote attackers to include arbitrary files via a .. (dot dot) in the (1) tema_dizin parameter to baslik.php and (2) portal_ayarlarportal_dili parameter to anket_yonetim.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-25	5.0	CVE-2008-6516 XF BID
phpmyadmin -- phpmyadmin	Directory traversal vulnerability in bs_disp_as_mime_type.php in the BLOB streaming feature in phpMyAdmin before 3.1.3.1 allows remote attackers to read arbitrary files via directory traversal sequences in the file_path parameter ($filename variable).	2009-03-26	5.0	CVE-2009-1148 CONFIRM
phpmyadmin -- phpmyadmin	Multiple cross-site scripting (XSS) vulnerabilities in the export page (display_export.lib.php) in phpMyAdmin 2.11.x before 2.11.9.5 and 3.x before 3.1.3.1 allow remote attackers to inject arbitrary web script or HTML via the pma_db_filename_template cookie.	2009-03-26	4.3	CVE-2009-1150 CONFIRM
piwik -- piwik	Piwik 0.2.32 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain the API key and other sensitive information via a direct request for misc/cron/archive.sh.	2009-03-25	5.0	CVE-2009-1085 MLIST MISC CONFIRM
rapidleech -- rapid_leech	Absolute path traversal vulnerability in upload.php in Rapidleech rev.36 and earlier allows remote attackers to read arbitrary files via a base64-encoded absolute path in the filename parameter.	2009-03-25	5.0	CVE-2009-1089 XF BID BUGTRAQ MISC SECUNIA
rapidleech -- rapidleech	Directory traversal vulnerability in upload.php in Rapidleech rev.36 and earlier allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the uploaded parameter.	2009-03-25	6.8	CVE-2009-1090 XF BID BUGTRAQ MISC SECUNIA OSVDB

rapidleech -- rapid_leech	Cross-site scripting (XSS) vulnerability in upload.php in Rapidleech rev.36 and earlier allows remote attackers to inject arbitrary web script or HTML via the uploaded parameter.	2009-03-25	4.3	CVE-2009-1091 XF BID BUGTRAQ MISC SECUNIA OSVDB
sitecore -- cms	Unspecified vulnerability in the web service in Sitecore CMS 5.3.1 rev. 071114 allows remote authenticated users to gain access to security databases, and obtain administrative and user credentials, via unknown vectors related to SOAP and XML requests.	2009-03-24	4.0	CVE-2009-1055 XF VUPEN BID BUGTRAQ SECUNIA CONFIRM
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 does not use SSL in all expected circumstances, which makes it easier for remote attackers to obtain sensitive information by sniffing the network, related to "ssl termination devices" and lack of support for relative URLs.	2009-03-25	5.0	CVE-2009-1074 CONFIRM CONFIRM
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 responds differently to failed use of the Forgot Password feature depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-03-25	5.0	CVE-2009-1075 SUNALERT CONFIRM CONFIRM
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 responds differently to failed use of the end-user question-based login feature depending on whether the user account exists, which allows remote attackers to enumerate valid usernames.	2009-03-25	5.0	CVE-2009-1076 BID CONFIRM CONFIRM
sun -- java_system_identity_manager	The Change My Password implementation in the admin interface in Sun Java System Identity Manager (IdM) 7.0 through 8.0 does not enforce the RequiresChallenge property setting, which allows remote authenticated users to change the passwords of other users, as demonstrated by changing the administrator's password.	2009-03-25	6.5	CVE-2009-1077 SUNALERT CONFIRM CONFIRM CONFIRM CONFIRM CONFIRM
	Sun Java System Identity Manager (IdM) 7.0 through 8.0 does not enforce the			CVE-2009-

sun -- java_system_identity_manager	expected privilege requirements for (1) deleting audit policies and (2) modifying workflows, which allows remote authenticated users to have an unspecified impact.	2009-03-25	4.0	1078 SUNALERT CONFIRM CONFIRM
sun -- java_system_identity_manager	Multiple cross-site scripting (XSS) vulnerabilities in Sun Java System Identity Manager (IdM) 7.0 through 8.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Bug IDs 19659, 19660, and 19683.	2009-03-25	4.3	CVE-2009-1079 SUNALERT CONFIRM
sun -- java_system_identity_manager	Multiple cross-site scripting (XSS) vulnerabilities in Sun Java System Identity Manager (IdM) 7.0 through 8.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Bug ID 19033.	2009-03-25	4.3	CVE-2009-1080 SUNALERT CONFIRM
sun -- java_system_identity_manager	Multiple cross-site scripting (XSS) vulnerabilities in Sun Java System Identity Manager (IdM) 7.0 through 8.0 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka Bug IDs 19595 and 19661.	2009-03-25	4.3	CVE-2009-1081 SUNALERT CONFIRM
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 on Linux, AIX, Solaris, and HP-UX permits "control characters" in the passwords of user accounts, which allows remote attackers to execute arbitrary commands via vectors involving "resource adapters."	2009-03-25	5.0	CVE-2009-1083 SUNALERT CONFIRM CONFIRM
sun -- java_system_identity_manager	Sun Java System Identity Manager (IdM) 7.0 through 8.0 does not properly restrict access to the System Configuration object, which allows remote authenticated administrators and possibly remote attackers to have an unspecified impact by modifying this object.	2009-03-25	6.4	CVE-2009-1084 SUNALERT CONFIRM CONFIRM CONFIRM
sun -- jdk sun -- jre	LdapCtx in the LDAP service in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier; 6 Update 12 and earlier; SDK and JRE 1.3.1_24 and earlier; and 1.4.2_19 and earlier does not close the connection when initialization fails, which allows remote attackers to cause a denial of service (LDAP service hang).	2009-03-25	5.0	CVE-2009-1093 SUNALERT MISC

sun -- jdk sun -- jre	Multiple unspecified vulnerabilities in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier, and 6 Update 12 and earlier, allow remote attackers to cause a denial of service (disk consumption) via vectors related to temporary font files and (1) "limits on Font creation," aka CR 6522586, and (2) another unspecified vector, aka CR 6632886.	2009-03-25	5.0	CVE-2009-1100 SUNALERT MISC
sun -- jdk sun -- jre	Unspecified vulnerability in the lightweight HTTP server implementation in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12 and earlier allows remote attackers to cause a denial of service (probably resource consumption) for a JAX-WS service endpoint via a connection without any data, which triggers a file descriptor "leak."	2009-03-25	6.4	CVE-2009-1101 SUNALERT MISC
sun -- java	Unspecified vulnerability in the Virtual Machine in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12 and earlier allows remote attackers to access files and execute arbitrary code via unknown vectors related to "code generation."	2009-03-25	6.4	CVE-2009-1102 SUNALERT
sun -- java	Unspecified vulnerability in the Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier; 6 Update 12 and earlier; 1.4.2_19 and earlier; and 1.3.1_24 and earlier allows remote attackers to access files and execute arbitrary code via unknown vectors related to "deserializing applets," aka CR 6646860.	2009-03-25	6.4	CVE-2009-1103 SUNALERT
sun -- java	The Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 5.0 Update 17 and earlier; 6 Update 12 and earlier; and 1.4.2_19 and earlier does not prevent Javascript that is loaded from the localhost from connecting to other ports on the system, which allows user-assisted attackers to bypass intended access restrictions via LiveConnect, aka CR 6724331. NOTE: this vulnerability	2009-03-25	5.8	CVE-2009-1104 SUNALERT MISC

	can be leveraged with separate cross-site scripting (XSS) vulnerabilities for remote attack vectors.			
sun -- jdk sun -- jre	The Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12, 11, and 10 does not properly parse crossdomain.xml files, which allows remote attackers to bypass intended access restrictions and connect to arbitrary sites via unknown vectors, aka CR 6798948.	2009-03-25	6.4	CVE-2009-1106 SUNALERT MISC
sun -- java	The Java Plug-in in Java SE Development Kit (JDK) and Java Runtime Environment (JRE) 6 Update 12 and earlier, and 5.0 Update 17 and earlier, allows remote attackers to trick a user into trusting a signed applet via unknown vectors that misrepresent the security warning dialog, related to a "Swing JLabel HTML parsing vulnerability," aka CR 6782871.	2009-03-25	4.3	CVE-2009-1107 SUNALERT MISC
tmaxsoft -- jeus	NTFS TmaxSoft JEUS 5 before Fix 26 allows remote attackers to read the source code for scripts by appending ::$DATA to the URL, which accesses the alternate data stream.	2009-03-26	5.0	CVE-2008-6528 XF BID BUGTRAQ BUGTRAQ MILW0RM SECUNIA
vclcomponents -- yappa-ng	Cross-site scripting (XSS) vulnerability in Fritz Berger yet another php photo album - next generation (yappa-ng) allows remote attackers to inject arbitrary web script or HTML via the query string to the default URI.	2009-03-24	4.3	CVE-2008-6515 BID MISC
videolan -- vlc_media_player	requests/status.xml in VLC 0.9.8a allows remote attackers to cause a denial of service (stack consumption and crash) via a long input argument in an in_play action.	2009-03-23	5.0	CVE-2009-1045 XF MLIST MILW0RM MISC
vidiscript -- vidiscript	Unrestricted file upload vulnerability in the profile feature in VidiScript allows registered remote authenticated users to execute arbitrary code by uploading a PHP file as an Avatar, then accessing the avatar via a direct request.	2009-03-25	6.5	CVE-2008-6518 XF BID MILW0RM

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openssl -- openssl	The CMS_verify function in OpenSSL 0.9.8h through 0.9.8j, when CMS is enabled, does not properly handle errors associated with malformed signed attributes, which allows remote attackers to repudiate a signature that originally appeared to be valid but was actually invalid.	2009-03-27	2.6	CVE-2009-0591 XF VUPEN BID OSVDB CONFIRM CONFIRM CONFIRM SECTRACK SECUNIA SECUNIA
systemtap -- system_tap	Race condition in the SystemTap stap tool 0.0.20080705 and 0.0.20090314 allows local users in the stapusr group to gain privileges via unknown vectors.	2009-03-25	3.3	CVE-2009-0784

Back to top