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**
8pussy -- octopussy	Unspecified vulnerability in Octopussy before 0.9.5.8 has unknown impact and attack vectors related to a "major security" vulnerability.	2009-03-31	10.0	CVE-2008-6566 OSVDB CONFIRM
apple -- mac_os_x microsoft -- windows vidalia-project -- vidalia_bundle	Vidalia bundle before 0.1.2.18, when running on Windows and Mac OS X, installs Privoxy with a configuration file (config.txt or config) that contains insecure (1) enable-remote-toggle and (2) enable-edit-actions settings, which allows remote attackers to bypass intended access restrictions and modify configuration.	2009-03-31	10.0	CVE-2007-6722 MLIST
apple -- mac_os_x microsoft -- windows vidalia-project -- vidalia_bundle	Vidalia bundle before 0.1.2.18, when running on Windows and Mac OS X, installs Privoxy with a configuration file (config.txt or config) that contains an insecure enable-remote-http-toggle setting, which allows remote attackers to bypass intended access restrictions and modify configuration.	2009-03-31	10.0	CVE-2007-6724 MLIST
apple -- mac_os_x apple -- mac_os_x_server	XNU 1228.9.59 and earlier on Apple Mac OS X 10.5.6 and earlier does not properly restrict interaction between user space and the HFS IOCTL handler, which allows local users to overwrite kernel memory and gain privileges by attaching an HFS+ disk image and performing certain steps involving HFS_GET_BOOT_INFO fcntl calls.	2009-04-02	7.2	CVE-2009-1235 VUPEN BID MILW0RM MISC MISC MISC
apple -- mac_os_x apple -- mac_os_x_server	Heap-based buffer overflow in the AppleTalk networking stack in XNU 1228.3.13 and earlier on Apple Mac OS X 10.5.6 and earlier allows remote attackers to cause a denial of service (system crash) via a ZIP NOTIFY (aka ZIPOP_NOTIFY) packet that overwrites a certain ifPort structure member.	2009-04-02	10.0	CVE-2009-1236 BID MILW0RM MISC MISC

apple -- mac_os_x apple -- mac_os_x_server	Race condition in the HFS vfs sysctl interface in XNU 1228.8.20 and earlier on Apple Mac OS X 10.5.6 and earlier allows local users to cause a denial of service (kernel memory corruption) by simultaneously executing the same HFS_SET_PKG_EXTENSIONS code path in multiple threads, which is problematic because of lack of mutex locking for an unspecified global variable.	2009-04-02	7.2	CVE-2009-1238 BID MILW0RM MISC MISC
arcadwy -- arcadwy_arcade_script	SQL injection vulnerability in Arcadwy Arcade Script allows remote attackers to execute arbitrary SQL commands via the user cookie parameter.	2009-04-02	7.5	CVE-2009-1229 MISC XF BID MILW0RM SECUNIA
auth2db -- auth2db auth2dbauth2db -- 0.1.1	SQL injection vulnerability in auth2db 0.2.5, and possibly other versions before 0.2.7, uses the addslashes function instead of the mysql_real_escape_string function, which allows remote attackers to conduct SQL injection attacks using multibyte character encodings.	2009-04-01	7.5	CVE-2009-1208 DEBIAN CONFIRM
avaya -- communication_manager	Unspecified vulnerability in SIP Enablement Services (SES) in Avaya Communication Manager 3.1.x and 4.x allows remote attackers to gain privileges and cause a denial of service via unknown vectors related to reuse of valid credentials.	2009-04-01	7.5	CVE-2008-6574 XF MISC BID SECUNIA OSVDB
aztech -- adsl2/2+4-port	cgi-bin/script in Aztech ADSL2/2+ 4-port router 3.7.0 build 070426 allows remote attackers to execute arbitrary commands via shell metacharacters in the query string.	2009-03-30	10.0	CVE-2008-6554 XF BID BUGTRAQ SECUNIA OSVDB
ceruleanstudios -- trillian	Buffer overflow in the XML parser in Trillian 3.1.9.0, and possibly earlier, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DTD file.	2009-03-31	9.3	CVE-2008-6563 XF BID BUGTRAQ OSVDB
checkpoint -- firewall-1_pki_web_service	Buffer overflow in the PKI Web Service in Check Point Firewall-1 PKI Web Service allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long (1) Authorization or (2) Referer HTTP header to TCP port 18624.	2009-04-02	7.5	CVE-2009-1227 SECTRACK BID BUGTRAQ MILW0RM FULLDISC
cisco -- ios	Memory leak in the Cisco Tunneling Control Protocol (cTCP) encapsulation feature in Cisco IOS 12.4, when an Easy VPN (aka EZVPN) server is enabled, allows remote attackers to cause a denial of service (memory consumption and device crash) via a sequence of TCP packets.	2009-03-27	7.1	CVE-2009-0635 CONFIRM CISCO
	Session fixation vulnerability in Cybozu Garoon 2.0.0 through	2009-03		CVE-2008-6569 BID MISC

cybozu -- garoon	2.1.3 allows remote attackers to hijack web sessions via the session ID in the login page.	2009-03-31	9.3	SECUNIA OSVDB JVNDB JVN CONFIRM
ezbsystems -- ultraiso	Multiple format string vulnerabilities in UltraISO 9.3.1.2633, and possibly other versions before 9.3.3.2685, allow user-assisted attackers to execute arbitrary code via format string specifiers in the filename of a (1) DAA or (2) ISZ file.	2009-04-01	9.3	CVE-2008-3871 MISC
ezbsystems -- ultraiso	Multiple buffer overflows in UltraISO 9.3.1.2633, and possibly other versions before 9.3.3.2685, allow user-assisted attackers to execute arbitrary code via a crafted (1) CIF, (2) C2D, or (3) GI file.	2009-04-01	9.3	CVE-2008-4825 MISC MISC SECUNIA
futomi -- cgi_cafe_access_analyzer_cgi	Unspecified vulnerability in futomi's CGI Cafe Access Analyzer CGI Professional Version 4.11.5 and earlier allows remote attackers to gain administrative privileges via unknown vectors.	2009-04-01	7.5	CVE-2009-1206 XF CONFIRM SECUNIA JVNDB JVN
ibm -- websphere_application_server	The JAX-RPC WS-Security runtime in the Web Services Security component in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.23 and 7.0 before 7.0.0.3, when APAR PK41002 is installed, does not properly validate UsernameToken objects, which has unknown impact and attack vectors.	2009-03-31	10.0	CVE-2009-1172 CONFIRM CONFIRM
ibm -- websphere_application_server	The Web Services Security component in IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.3 has an unspecified "security problem" in the XML digital-signature specification, which has unknown impact and attack vectors.	2009-03-31	10.0	CVE-2009-1174 CONFIRM
ibm -- tivoli_storage_manager	Unspecified vulnerability in the server in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.2 and 6.x before 6.1 has unknown impact and attack vectors related to the "admin command line."	2009-03-31	10.0	CVE-2009-1178 CONFIRM
ibm -- db2_content_manager	Unspecified vulnerability in the eClient in IBM DB2 Content Manager 8.4.1 before 8.4.1.1 has unknown impact and attack vectors.	2009-04-02	10.0	CVE-2009-1231 CONFIRM
ixprim-cms -- ixprim	PHP remote file inclusion vulnerability in mod/nc_phpmyadmin/core/libraries/Theme_Manager.class.php in Ixprim 2.0 allows remote attackers to execute arbitrary PHP code via a URL in an unspecified parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-31	7.5	CVE-2006-7237 XF BID MISC
microsoft -- subsystem_for_unix-based_applications microsoft -- windows_services_for_unix microsoft -- windows_server_2008 microsoft -- windows_vista	Multiple unspecified vulnerabilities in (1) unlzh.c and (2) unpack.c in the gzip libraries in Microsoft Windows Server 2008, Windows Services for UNIX 3.0 and 3.5, and the Subsystem for UNIX-based Applications (SUA); as used in gunzip, gzip, pack, pcat, and unpack 7.x before 7.0.1701.48, 8.x before 8.0.1969.62, and 9.x before 9.0.3790.2076; allow remote attackers to execute arbitrary code via unknown vectors.	2009-04-01	10.0	CVE-2009-1216 XF VUPEN MSKB SECTRACK SECUNIA
	SQL injection vulnerability in index.php in Miniweb 2.0	2009-04		CVE-2008-6582 XF

miniweb2 -- miniweb	allows remote attackers to execute arbitrary SQL commands via the username parameter in a login action.	2009-04-02	7.5	XF BID MILW0RM SECUNIA
nortel -- communication_server_1000 nortel -- unistim_protocol	Nortel UNIStim protocol, as used in Communication Server 1000 and other products, uses predictable sequence numbers, which allows remote attackers to hijack sessions via sniffing or brute force attacks.	2009-03-31	7.6	CVE-2008-6564 XF MISC SECTRACK CONFIRM OSVDB
nortel -- cs1000	Unspecified vulnerability in the "session limitation technique" in the FTP service on Nortel Communications Server 1000 (CS1K) 4.50.x, when running on VGMC or signaling nodes, allows remote attackers to cause a denial of service (resource exhaustion and failed updates) via unknown vectors that causes consumption of all available sessions.	2009-04-01	7.8	CVE-2008-6576 XF MISC CONFIRM SECTRACK
nortel -- cs1000	Nortel MG1000S, Signaling Server, and Call Server on the Communications Server 1000 (CS1K) 4.50.x contain multiple unspecified hard-coded accounts and passwords, which allows remote attackers to gain privileges.	2009-04-01	10.0	CVE-2008-6577 XF CONFIRM SECTRACK
nortel -- cs1000	Multiple unspecified vulnerabilities in Nortel Communication Server 1000 4.50.x allow remote attackers to execute arbitrary commands to gain privileges, obtain sensitive information, or cause a denial of service via unknown vectors.	2009-04-01	10.0	CVE-2008-6578 XF CONFIRM SECTRACK
phpaddedit -- phpaddedit	login.php in PhpAddEdit 1.3 allows remote attackers to bypass authentication and gain administrative access by setting the addedit cookie parameter.	2009-04-02	7.5	CVE-2008-6581 CONFIRM
podcast_generator -- podcast_generator	core/admin/delete.php in Podcast Generator 1.1 and earlier does not properly restrict access to administrative functions, which allows remote attackers to delete arbitrary files via the file parameter.	2009-04-02	7.5	CVE-2009-1226 BID MILW0RM SECUNIA
precisionid -- data_matrix_barcode_activex_control	Multiple insecure method vulnerabilities in PRECIS~2.DLL in the PrecisionID Datamatrix ActiveX control (DMATRIXLib.Datamatrix) allow remote attackers to overwrite arbitrary files via the (1) SaveBarCode and (2) SaveEnhWMF methods.	2009-04-01	7.8	CVE-2009-1212 BUGTRAQ MILW0RM MISC
puppet_master -- webutil	cgi-bin/webutil.pl in The Puppet Master WebUtil 2.3 allows remote attackers to execute arbitrary commands via shell metacharacters in the whois command.	2009-03-30	10.0	CVE-2008-6556 XF BID BUGTRAQ OSVDB
puppetmaster -- webutil	cgi-bin/webutil.pl in The Puppet Master WebUtil allows remote attackers to execute arbitrary commands via shell metacharacters in the dig command.	2009-03-30	10.0	CVE-2008-6555 XF BID BUGTRAQ OSVDB
puppetmaster -- webutil	cgi-bin/webutil.pl in The Puppet Master WebUtil 2.7 allows remote attackers to execute arbitrary commands via shell	2009-03-30	10.0	CVE-2008-6557 XF BID

	metacharacters in the details command.	30		BID BUGTRAQ OSVDB
redhat -- cman	Buffer overflow in CMAN - The Cluster Manager before 2.03.09-1 on Fedora 9 and Red Hat Enterprise Linux (RHEL) 5 allows attackers to cause a denial of service (CPU consumption and memory corruption) via a cluster.conf file with many lines. NOTE: it is not clear whether this issue crosses privilege boundaries in realistic uses of the product.	2009-03-31	7.8	CVE-2008-6560 CONFIRM FEDORA FEDORA FEDORA CONFIRM
sap -- sapgui	Stack-based buffer overflow in EAI WebViewer3D ActiveX control (webviewer3d.dll) in SAP AG SAPgui before 7.10 Patch Level 9 allows remote attackers to execute arbitrary code via a long argument to the SaveViewToSessionFile method.	2009-04-01	9.3	CVE-2007-4475 CERT-VN MISC
scivox -- vsp_stats_processor	SQL injection vulnerability in vsp-core/pub/themes/bismarck/gamestat.php in vsp stats processor 0.45 allows remote attackers to execute arbitrary SQL commands via the gameID parameter.	2009-04-02	7.5	CVE-2009-1224 MILW0RM
sco -- reliantha	Merge mcd in ReliantHA 1.1.4 in SCO UnixWare 7.1.4 allows local users to gain root privileges via a crafted -d argument that contains .. (dot dot) sequences that point to a directory containing a file whose name includes shell metacharacters.	2009-03-30	7.2	CVE-2008-6559 BID
trendmicro -- internet_security	The TrendMicro Activity Monitor Module (tmactmon.sys) 2.52.0.1002 in Trend Micro Internet Pro 2008 and 2009, and Security Pro 2008 and 2009, allows local users to gain privileges via a crafted IRP in a METHOD_NEITHER IOCTL request to \Device\tmactmon that overwrites memory.	2009-04-01	7.2	CVE-2009-0686 XF BID BUGTRAQ MILW0RM MISC MISC
umn -- mapserver	Stack-based buffer overflow in mapserv.c in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2, when the server has a map with a long IMAGEPATH or NAME attribute, allows remote attackers to execute arbitrary code via a crafted id parameter in a query action.	2009-03-31	10.0	CVE-2009-0839 SECTRACK BID BUGTRAQ MISC CONFIRM MLIST
umn -- mapserver	Heap-based buffer underflow in the readPostBody function in cgiutil.c in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2 allows remote attackers to have an unknown impact via a negative value in the Content-Length HTTP header.	2009-03-31	10.0	CVE-2009-0840 MLIST
umn -- mapserver	Directory traversal vulnerability in mapserv.c in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2, when running on Windows with Cygwin, allows remote attackers to create arbitrary files via a .. (dot dot) in the id parameter.	2009-03-31	10.0	CVE-2009-0841 MLIST
umn -- mapserver	The msLoadQuery function in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2 allows remote attackers to determine the existence of arbitrary files via a full pathname in the queryfile parameter, which triggers different error messages depending on whether this pathname exists.	2009-03-31	7.8	CVE-2009-0843 MLIST
	mapserv.c in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2 does not ensure that the string holding the id			CVE-2009

umn -- mapserver	parameter ends in a '\0' character, which allows remote attackers to conduct buffer-overflow attacks or have unspecified other impact via a long id parameter in a query action.	2009-03-31	10.0	CVE-2009-1176 MLIST
umn -- mapserver	Multiple stack-based buffer overflows in maptemplate.c in mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2 have unknown impact and remote attack vectors.	2009-03-31	10.0	CVE-2009-1177 MLIST
w3 -- amaya	Stack-based buffer overflow in W3C Amaya Web Browser 11.1 allows remote attackers to execute arbitrary code via a script tag with a long defer attribute.	2009-04-01	9.3	CVE-2009-1209 BID MILW0RM MILW0RM SECUNIA
wireshark -- wireshark	Format string vulnerability in the PROFINET/DCP (PN-DCP) dissector in Wireshark 1.0.6 and earlier allows remote attackers to execute arbitrary code via a PN-DCP packet with format string specifiers in the station name. NOTE: some of these details are obtained from third party information.	2009-04-01	10.0	CVE-2009-1210 XF BID MILW0RM SECUNIA
yehe -- yehe	Unrestricted file upload vulnerability in Yehe 2.0 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 the envoyer feature. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-31	10.0	CVE-2008-6568 XF BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
abledating -- abledating	SQL injection vulnerability in search_results.php in ABK-Soft AbleDating 2.4 allows remote attackers to execute arbitrary SQL commands via the keyword parameter.	2009-03-31	6.8	CVE-2008-6572 XF BID BUGTRAQ SECUNIA
anonymityanywhere -- tork	TorK before 0.22, when running on Windows and Mac OS X, installs Privoxy with a configuration file (config.txt or config) that contains insecure (1) enable-remote-toggle and (2) enable-edit-actions settings, which allows remote attackers to bypass intended access restrictions and modify configuration.	2009-03-31	4.3	CVE-2007-6723 XF BID OSVDB CONFIRM MLIST MLIST
apple -- safari	Apple Safari 3.2.2 and 4 Beta on Windows allows remote attackers to cause a denial of service (application crash) via an XML document containing many nested A elements.	2009-04-02	4.3	CVE-2009-1233 XF BID MILW0RM
apple -- mac_os_x apple -- mac_os_x_server	Multiple memory leaks in XNU 1228.3.13 and earlier on Apple Mac OS X 10.5.6 and earlier allow local users to cause a denial of service (kernel memory consumption) via a crafted (1)	2009-04-02	4.9	CVE-2009-1237 BID MILW0RM MILW0RM MISC

	SYS_add_profil or (2) SYS___mac_getfsstat system call.			MISC MISC MISC
arcadwy -- arcadwy_arcade_script_cms	Cross-site scripting (XSS) vulnerability in register.php in Arcadwy Arcade Script CMS allows remote attackers to inject arbitrary web script or HTML via the username field (user_name parameter).	2009-04-02	4.3	CVE-2009-1228 XF BID MILW0RM SECUNIA
avaya -- communication_manager	Multiple SQL injection vulnerabilities in Avaya SIP Enablement Services (SES) in Avaya Avaya Communication Manager 3.x, 4.0, and 5.0 (1) allow remote attackers to execute arbitrary SQL commands via unspecified vectors related to profiles in the SIP Personal Information Manager (SPIM) in the web interface; and allow remote authenticated users to execute arbitrary SQL commands via unspecified vectors related to (2) permissions for SPIM profiles in the web interface and (3) a crafted SIP request to the SIP server.	2009-04-01	6.8	CVE-2008-6573 XF XF MISC MISC MISC BID CONFIRM CONFIRM SECUNIA OSVDB OSVDB OSVDB
avaya -- communication_manager	Unspecified vulnerability in the SIP server in SIP Enablement Services (SES) in Avaya Communication Manager 3.1.x and 4.x allows remote authenticated users to cause a denial of service (resource consumption) via unknown vectors.	2009-04-01	6.8	CVE-2008-6575 XF MISC SECUNIA OSVDB
banshee-project -- banshee	Cross-site scripting (XSS) vulnerability in apps/web/vs_diag.cgi in the DAAP extension in Banshee 1.4.2 allows remote attackers to inject arbitrary web script or HTML via the server parameter, which is not properly handled in an error message.	2009-03-31	4.3	CVE-2009-1175 MLIST CONFIRM
bluecoat -- proxysg	Blue Coat ProxySG, when transparent interception mode is enabled, uses the HTTP Host header to determine the remote endpoint, which allows remote attackers to bypass access controls for Flash, Java, Silverlight, and probably other technologies, and possibly communicate with restricted intranet sites, via a crafted web page that causes a client to send HTTP requests with a modified Host header.	2009-04-01	5.8	CVE-2009-1211 CONFIRM SECTRACK
cisco -- adaptive_security_appliance cisco -- ios	Cross-site scripting (XSS) vulnerability in +webvpn+/index.html in WebVPN on the Cisco Adaptive Security Appliances (ASA) 5520 with software 7.2(2)22 allows remote attackers to inject arbitrary web script or HTML via the Host HTTP header.	2009-04-01	4.3	CVE-2009-1220 XF BID BUGTRAQ FULLDISC
	Cross-site scripting (XSS) vulnerability in			CVE-2008-6570 BID

cybozu -- garoon	the RSS reader in Cybozu Garoon 2.0.0 through 2.1.3 allows remote attackers to inject arbitrary web script or HTML via a crafted RSS feed.	2009-03-31	4.3	MISC SECUNIA OSVDB JVNDB JVN CONFIRM
debian -- nss-ldap	nss-ldapd before 0.6.8 uses world-readable permissions for the /etc/nss-ldapd.conf file, which allows local users to obtain a cleartext password for the LDAP server by reading the bindpw field.	2009-03-31	4.9	CVE-2009-1073 DEBIAN CONFIRM
fullrevolution -- aspwebcalendar	aspWebCalendar Free Edition 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 calendar/calendar.mdb.	2009-04-02	5.0	CVE-2009-1223 BUGTRAQ
funscripts -- red_reservations	The Red_Reservations script for ColdFusion stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database via a direct request to (1) makered.mdb and (2) makered97.mdb.	2009-04-02	5.0	CVE-2008-6580 MILW0RM
gallarific -- gallarific	Multiple cross-site scripting (XSS) vulnerabilities in Gallarific Free Edition allow remote attackers to inject arbitrary web script or HTML via (1) the e-mail address, (2) a comment, which is not properly handled during moderation, and (3) the tag parameter to gallery/tags.php.	2009-03-31	4.3	CVE-2008-6567 BID OSVDB OSVDB OSVDB FULLDISC
gnu -- screen	GNU screen 4.0.3 creates the /tmp/screen-exchange temporary file with world-readable permissions, which might allow local users to obtain sensitive session information.	2009-04-01	4.9	CVE-2009-1214 CONFIRM CONFIRM MLIST MISC CONFIRM
ibm -- websphere_application_server	The administrative console in IBM WebSphere Application Server (WAS) 6.1 before 6.1.0.23 and 7.0 before 7.0.0.3 allows attackers to hijack user sessions in "specific scenarios" related to a forced logout.	2009-03-31	5.5	CVE-2009-0892 CONFIRM CONFIRM
ibm -- tivoli_storage_manager	The server in IBM Tivoli Storage Manager (TSM) 4.2.x on MVS, 5.1.9.x before 5.1.9.1, 5.1.x before 5.1.10, 5.2.2.x before 5.2.2.3, 5.2.x before 5.2.3, 5.3.x before 5.3.0, and 6.x before 6.1, when the HTTP communication method is enabled, allows remote attackers to cause a denial of service (daemon crash or hang) via unspecified HTTP traffic, as demonstrated by the IBM port scanner 1.3.1.	2009-03-31	4.3	CVE-2004-2762 VUPEN BID AIXAPAR CONFIRM CONFIRM SECTRACK SECUNIA
	Cross-site scripting (XSS) vulnerability in			CVE-2008-

invision_power_services -- invision_power_board	Invision Power Board 2.3.1 and earlier allows remote attackers to inject arbitrary web script or HTML via an IFRAME tag in the signature.	2009-03-31	4.3	6565 XF BID BUGTRAQ
jax_scripts -- jax_guestbook	Multiple cross-site scripting (XSS) vulnerabilities in jax_guestbook.php in Jax Guestbook 3.1 and 3.31 allow remote attackers to inject arbitrary web script or HTML via the (1) gmt_ofs and (2) language parameters. NOTE: the page parameter is already covered by CVE-2006-1913. NOTE: it was later reported that 3.50 is also affected.	2009-03-31	4.3	CVE-2005-4879 BID SECUNIA MISC MISC
jax_scripts -- jax_guestbook	Jax Guestbook 3.1 and 3.31 stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain IP addresses of users via a direct request to (1) guestbook, (2) guestbook_ips2block, (3) ips2block, and (4) formmailer/logfile.csv.	2009-03-31	5.0	CVE-2005-4880 SECUNIA MISC
jax_scripts -- jax_linklists	Cross-site scripting (XSS) vulnerability in jax_linklists.php in Jack (tR) Jax LinkLists 1.00 allows remote attackers to inject arbitrary web script or HTML via the cat parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-03-31	4.3	CVE-2008-6562 XF BID
linpha -- linpha	Multiple cross-site scripting (XSS) vulnerabilities in LinPHA before 1.3.4 might allow remote attackers to inject arbitrary web script or HTML via (1) new_images.php, (2) login.php, and unspecified vectors.	2009-03-31	4.3	CVE-2008-6571 SECUNIA OSVDB OSVDB OSVDB CONFIRM
living-e -- webedition	Directory traversal vulnerability in index.php in webEdition 6.0.0.4 and earlier, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary files via a .. (dot dot) in the WE_LANGUAGE parameter.	2009-04-02	5.1	CVE-2009-1222 XF BID BUGTRAQ MILW0RM SECUNIA
microsoft -- gdiplus microsoft -- windows_xp	Off-by-one error in the GpFont::SetData function in gdiplus.dll in Microsoft GDI+ on Windows XP allows remote attackers to cause a denial of service (stack corruption and application termination) via a crafted EMF file that triggers an integer overflow, as demonstrated by voltage-exploit.emf, aka the "Microsoft GdiPlus EMF GpFont.SetData integer overflow."	2009-04-01	4.3	CVE-2009-1217 XF VUPEN CONFIRM MISC
	The spnego_gss_accept_sec_context function in			CVE-2009-0845 XF

mit -- kerberos	lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.6.3, when SPNEGO is used, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via invalid ContextFlags data in the reqFlags field in a negTokenInit token.	2009-03-27	5.0	XF VUPEN BID MANDRIVA CONFIRM CONFIRM SECUNIA CONFIRM
moodle -- moodle	The TeX filter in Moodle 1.6 before 1.6.9+, 1.7 before 1.7.7+, 1.8 before 1.8.9, and 1.9 before 1.9.5 allows user-assisted attackers to read arbitrary files via an input command in a "$$" sequence, which causes LaTeX to include the contents of the file.	2009-03-30	4.3	CVE-2009-1171 MILW0RM CONFIRM
mozilla -- bugzilla	Cross-site request forgery (CSRF) vulnerability in attachment.cgi in Bugzilla 3.2 before 3.2.3, 3.3 before 3.3.4, and earlier versions allows remote attackers to hijack the authentication of arbitrary users for requests that use attachment editing.	2009-04-01	6.8	CVE-2009-1213 VUPEN CONFIRM
mozilla -- firefox	The XUL parser in Mozilla Firefox 3.0.8 and earlier 3.0.x versions allows remote attackers to cause a denial of service (memory corruption) via an XML document composed of a long series of start-tags with no corresponding end-tags.	2009-04-02	4.3	CVE-2009-1232 XF MILW0RM MISC
nortel -- cs1000	Nortel Communication Server 1000 4.50.x allows remote attackers to obtain Web application structure via unknown vectors related to "web resources to phones and administrators."	2009-04-01	5.0	CVE-2008-6579 XF MISC CONFIRM SECTRACK
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
openswan -- openswan strongswan -- strongswan	The pluto IKE daemon in Openswan and Strongswan IPsec 2.6 before 2.6.21 and 2.4 before 2.4.14, and Strongswan 4.2 before 4.2.14 and 2.8 before 2.8.9, allows remote attackers to cause a denial of service (daemon crash and restart) via a crafted (1) R_U_THERE or (2) R_U_THERE_ACK Dead Peer Detection (DPD) IPsec IKE Notification message that triggers a NULL pointer dereference related to inconsistent ISAKMP state and the lack of a phase2 state association in DPD.	2009-04-01	5.0	CVE-2009-0790 BID DEBIAN DEBIAN
opera -- opera	Opera 9.64 allows remote attackers to cause a denial of service (application crash) via an XML document containing a	2009-04-02	4.3	CVE-2009-1234 XF

	long series of start-tags with no corresponding end-tags.	02		BID MILW0RM
platinumprofitzone -- turnkey_ebook_store	Cross-site scripting (XSS) vulnerability in index.php in Turnkey Ebook Store 1.1 allows remote attackers to inject arbitrary web script or HTML via the keywords parameter in a search action.	2009-04-02	4.3	CVE-2009-1225 SECUNIA MISC
podcast_generator -- podcast_generator	Static code injection vulnerability in index.php in Podcast Generator 1.1 and earlier allows remote authenticated administrators to inject arbitrary PHP code into config.php via the recent parameter in a config change action.	2009-04-02	6.5	CVE-2009-1230 MILW0RM
redhat -- cluster_project redhat -- cman redhat -- gfs2-utils redhat -- rgmanager fedoraproject -- fedora	Red Hat Cluster Project 2.x allows local users to modify or overwrite arbitrary files via symlink attacks on files in /tmp, involving unspecified components in Resource Group Manager (aka rgmanager) before 2.03.09-1, gfs2-utils before 2.03.09-1, and CMAN - The Cluster Manager before 2.03.09-1 on Fedora 9.	2009-03-30	6.9	CVE-2008-6552 XF BID FEDORA FEDORA FEDORA SECUNIA
sco -- unixware unixware -- reliantha	Untrusted search path vulnerability in (1) hvdisp and (2) rcvm in ReliantHA 1.1.4 in SCO UnixWare 7.1.4 allows local users to gain root privileges by modifying the RELIANT_PATH environment variable to point to a malicious bin/hvenv program.	2009-03-30	6.2	CVE-2008-6558 SCO
sun -- opensolaris	Unspecified vulnerability in Sun OpenSolaris snv_100 through snv_101 allows local users, with privileges in a non-global zone, to execute arbitrary code in the global zone when a global-zone user is using mdb on a non-global zone process.	2009-03-30	6.9	CVE-2009-1170 XF VUPEN SECTRACK BID SUNALERT
sun -- solaris_10_sparc sun -- solaris_10_x86 sun -- solaris_8_sparc sun -- solaris_8x86 sun -- solaris_9_sparc sun -- solaris_9_x86 sun -- opensolaris	Race condition in the dircmp script in Sun Solaris 8 through 10, and OpenSolaris snv_01 through snv_111, allows local users to overwrite arbitrary files, probably involving a symlink attack on temporary files.	2009-04-01	4.7	CVE-2009-1207 MISC
sun -- java_system_calendar_server sun -- one_calendar_server	Multiple cross-site scripting (XSS) vulnerabilities in Sun Calendar Express Web Server in Sun ONE Calendar Server 6.0 and Sun Java System Calendar Server 6 2004Q2 through 6.3-7.01 allow remote attackers to inject arbitrary web script or HTML via (1) the fmt-out parameter to login.wcap or (2) the date parameter to command.shtml.	2009-04-01	4.3	CVE-2009-1218 SUNALERT
sun -- java_system_calendar_server sun -- one_calendar_server	Sun Calendar Express Web Server in Sun ONE Calendar Server 6.0 and Sun Java System Calendar Server 6 2004Q2 through 6.3-7.01 allows remote attackers to cause a denial of service (daemon crash) via	2009-04-01	5.0	CVE-2009-1219 SUNALERT

	multiple requests to the default URI with alphabetic characters in the tzid parameter.			
tikiwiki -- tikiwiki_cms/groupware	Cross-site scripting (XSS) vulnerability in TikiWiki (Tiki) CMS/Groupware 2.2 allows remote attackers to inject arbitrary web script or HTML via the PHP_SELF portion of a URI to (1) tiki-galleries.php, (2) tiki-list_file_gallery.php, (3) tiki-listpages.php, and (4) tiki-orphan_pages.php.	2009-03-31	4.3	CVE-2009-1204 CONFIRM CONFIRM
umn -- mapserver	mapserv in MapServer 4.x before 4.10.4 and 5.x before 5.2.2 allows remote attackers to read arbitrary invalid .map files via a full pathname in the map parameter, which triggers the display of partial file contents within an error message, as demonstrated by a /tmp/sekrut.map symlink.	2009-03-31	4.3	CVE-2009-0842 MLIST
webwizguide -- web_wiz_guestbook	Web Wiz Guestbook 6.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database and obtain sensitive information via a direct request for database/WWGguestbook.mdb. NOTE: it was later reported that 8.21 is also affected.	2009-04-02	5.0	CVE-2003-1571 OSVDB MILW0RM MISC SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
citrix -- presentation_server_client	Citrix Presentation Server Client for Windows before 10.200 does not clear "credential information" from process memory in unspecified circumstances, which might allow local users to gain privileges.	2009-03-31	1.9	CVE-2008-6561 CONFIRM
gnu -- gnu_screen	Race condition in GNU screen 4.0.3 allows local users to create or overwrite arbitrary files via a symlink attack on the /tmp/screen-exchange temporary file.	2009-04-01	1.9	CVE-2009-1215 CONFIRM CONFIRM MLIST MISC CONFIRM
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 7.0 before 7.0.0.3 uses weak permissions (777) for files associated with unspecified "interim fixes," which allows attackers to modify files that would not have been accessible if the intended 755 permissions were used.	2009-03-31	2.1	CVE-2009-1173 CONFIRM
	The server in IBM Tivoli Storage Manager (TSM) 5.1.x, 5.2.x before 5.2.1.2, and 6.x before 6.1 does not require credentials to			CVE-2003-1570 VUPEN

ibm -- tivoli_storage_manager	observe the server console in some circumstances, which allows remote authenticated administrators to monitor server operations by establishing a console mode session, related to "session exposure."	2009-03-31	3.5	VUPEN BID AIXAPAR CONFIRM SECTRACK SECUNIA

Back to top