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**	**Sou Patc**
advantech -- adam-6015 advantech -- adam-6017 advantech -- adam-6018 advantech -- adam-6022 advantech -- adam-6024 advantech -- adam-6050 advantech -- adam-6050w advantech -- adam-6051 advantech -- adam-6051w advantech -- adam-6052 advantech -- adam-6060 advantech -- adam-6060w advantech -- adam-6066 advantech -- adam-6501	The Advantech ADAM-6000 module has 00000000 as its default password, which makes it easier for remote attackers to obtain access through an HTTP session, and (1) monitor or (2) control the module's Modbus/TCP I/O activity.	2009-01-06	10.0	CVE 5848 MIS(CON MIS(
apple -- safari	Integer signedness error in Apple Safari allows remote attackers to read the contents of arbitrary memory locations, cause a denial of service (application crash), and probably have unspecified other impact via the array index of the arguments array in a JavaScript	2009-01-08	9.3	CVE 0070 MIL'

	function, possibly a related issue to CVE-2008-2307.			
ca -- service_level_management ca -- service_metric_analysis	The smmsnmpd service in CA Service Metric Analysis r11.0 through r11.1 SP1 and Service Level Management 3.5 does not properly restrict access, which allows remote attackers to execute arbitrary commands via unspecified vectors.	2009-01-08	10.0	CVE 0043 CON BID
checkpoint -- vpn-1	** UNVERIFIABLE ** NOTE: this issue describes a problem that can not be independently verified as of 20090109. Unspecified vulnerability in the SmartCenter server for Check Point VPN-1 R55 through R65, as used in SecurePlatform, allows remote attackers to change the admin and expert passwords, and possibly have other impact, via unknown vectors involving a TCP session on the Check Point Management Interface (CPMI) port (18190/tcp), aka "SPLAT Remote Root Exploit." NOTE: this issue has no actionable details and was disclosed by a person of unknown reliability who did not coordinate with the vendor. The vendor has not indicated that they are aware of any vulnerability. As of 20090109, there has not been an independent public confirmation of this issue by a reliable party. CVE has no additional information regarding whether the original claim was valid or not.	2009-01-06	10.0	CVE 5850 MISC MLIS FULL
citrix -- broadcast_server citrix -- application_gateway	SQL injection vulnerability in login.asp in Citrix Application Gateway - Broadcast Server (BCS) before 6.1, as used by Avaya AG250 - Broadcast Server before 2.0 and possibly other products, allows remote attackers to execute arbitrary SQL commands via the txtUID parameter.	2009-01-09	7.5	CVE 5882 BID BUG CON
	Multiple heap-based buffer overflows in the AddTab method in the (1) Tab and (2) CTab ActiveX			CVE 4827 XF

componentone -- sizerone sap -- sap_gui sap -- tabone servantix -- tsc2_help_desk	controls in c1sizer.ocx and the (3) TabOne ActiveX control in sizerone.ocx in ComponentOne SizerOne 8.0.20081.140, as used in ComponentOne Studio for ActiveX 2008, TSC2 Help Desk 4.1.8, SAP GUI 6.40 Patch 29 and 7.10, and possibly other products, allow remote attackers to execute arbitrary code by adding many tabs, or adding tabs with long tab captions.	2009-01-08	9.3	XF XF BID BUG SECT MISC MISC MISC SECU SECU SECU
gobbl -- gobbl_cms	admin/auth.php in Gobbl CMS 1.0 allows remote attackers to bypass authentication and gain administrative access by setting the auth cookie to "ok".	2009-01-08	7.5	CVE 5880 BID MILW SECU
goople_cms -- goople_cms	SQL injection vulnerability in frontpage.php in Goople CMS 1.8.2 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter.	2009-01-09	7.5	CVE 0111 BID MILW SECU
hp -- openview_network_node_manager	Multiple stack-based buffer overflows in HP OpenView Network Node Manager (OV NNM) 7.51 allow remote attackers to execute arbitrary code via (1) long string parameters to the OpenView5.exe CGI program; (2) a long string parameter to the OpenView5.exe CGI program, related to ov.dll; or a long string parameter to the (3) getcvdata.exe, (4) ovlaunch.exe, or (5) Toolbar.exe CGI program.	2009-01-08	10.0	CVE 0067 BID BUG SECT MISC SECU
intel -- trusted_execution_technology	Multiple unspecified vulnerabilities in Intel system software for Trusted Execution Technology (TXT) allow attackers to bypass intended loader integrity protections, as demonstrated by exploitation of tboot. NOTE: as of 20090107, the only disclosure is a vague pre-advisory with no actionable information. However, because it is from a well-known researcher, it is being assigned a CVE identifier for tracking purposes.	2009-01-07	7.6	CVE 0066 BID MISC MISC MISC
	Stack-based buffer overflow in IntelliTamper 2.07 and 2.08 allows			

intellitamper -- intellitamper	user-assisted attackers to execute arbitrary code via a long ProxyLogin value in a configuration (.cfg) file.	2009-01-08	9.3	CVE 5868 MILV
invisible-island -- xterm	The default configuration of xterm on Debian GNU/Linux sid and possibly Ubuntu enables the allowWindowOps resource, which allows user-assisted attackers to execute arbitrary code or have unspecified other impact via escape sequences.	2009-01-02	9.3	CVE 7236 CON CON
invisible-island -- xterm	CRLF injection vulnerability in xterm allows user-assisted attackers to execute arbitrary commands via LF (aka \n) characters surrounding a command name within a Device Control Request Status String (DECRQSS) escape sequence in a text file, a related issue to CVE-2003-0063 and CVE-2003-0071.	2009-01-02	9.3	CVE 2383 FED FED SECU SECU CON
irrlicht -- irrlicht	Buffer overflow in Irrlicht before 1.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors in the B3D loader.	2009-01-08	9.3	CVE 5876 BID
joomlahbs -- com_tophotelmodule joomlahbs -- hotel_booking_reservation_system	SQL injection vulnerability in the Top Hotel (com_tophotelmodule) component 1.0 in the Hotel Booking Reservation System (aka HBS) 1.0.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a showhoteldetails action to index.php.	2009-01-06	7.5	CVE 5864 BID MILV
joomlahbs -- hotel_booking_reservation_system	SQL injection vulnerability in the com_hbssearch component 1.0 in the Hotel Booking Reservation System (aka HBS) 1.0.0 for Joomla! allows remote attackers to execute arbitrary SQL commands via the r_type parameter in a showhoteldetails action to index.php.	2009-01-06	7.5	CVE 5865 BID MILV SECU
	Multiple SQL injection vulnerabilities in the Hotel Booking Reservation System (aka HBS) for			

joomlahbs -- com_5starhotels joomlahbs -- com_allhotels joomlahbs -- hotel_booking_reservation_system	Joomla! allow remote attackers to execute arbitrary SQL commands via the id parameter in a showhoteldetails action to index.php in the (1) com_allhotels or (2) com_5starhotels module. NOTE: some of these details are obtained from third party information.	2009-01-08	7.5	CVE 5874 BID MISC
joomlahbs -- com_lowcosthotels joomlahbs -- hotel_booking_reservation_system	SQL injection vulnerability in the com_lowcosthotels component in the Hotel Booking Reservation System (aka HBS) for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a showhoteldetails action to index.php.	2009-01-08	7.5	CVE 5875 BID BUG
linux -- kernel	Buffer overflow in net/sctp/sm_statefuns.c in the Stream Control Transmission Protocol (sctp) implementation in the Linux kernel before 2.6.28-git8 allows remote attackers to have an unknown impact via an FWD-TSN (aka FORWARD-TSN) chunk with a large stream ID.	2009-01-07	10.0	CVE 0065 CON BID MLIS FRSI CON CON
mypbs -- mypbs	SQL injection vulnerability in index.php in My PHP Baseball Stats (MyPBS) allows remote attackers to execute arbitrary SQL commands via the seasonID parameter.	2009-01-06	7.5	CVE 5851 XF BID MILW
nortel -- multimedia_communication_server_5100	Multiple unspecified vulnerabilities in the UNIStim File Transfer Protocol (UFTP) processing in IP Client Manager (IPCM) in Nortel Multimedia Communication Server (MSC) 5100 3.0.13 allow remote attackers to cause a denial of service (device outage) via a UFTP message that has a negative block size or other crafted Connection Details values.	2009-01-08	7.8	CVE 5872 XF BID FRSI MISC CON SECU
php -- php	PHP 5.2.7 contains an incorrect change to the FILTER_UNSAFE_RAW functionality, and unintentionally disables magic_quotes_gpc regardless of the actual magic_quotes_gpc setting, which	2009-01-05	7.5	CVE 5844 SECT CON CON

	might make it easier for context-dependent attackers to conduct SQL injection attacks and unspecified other attacks.			CON CON
phpauctions -- phpauctions	SQL injection vulnerability in profile.php in PHPAuctions (aka PHPAuctionSystem) allows remote attackers to execute arbitrary SQL commands via the user_id parameter.	2009-01-09	7.5	CVE 0106 BID SECI OSV MILV
phpauctions -- phpauctions	PHPAuctions (aka PHPAuctionSystem) allows remote attackers to bypass authentication and gain administrative access via modified (1) PHPAUCTION_RM_ID, (2) PHPAUCTION_RM_NAME, (3) PHPAUCTION_RM_USERNAME, and (4) PHPAUCTION_RM_EMAIL cookies.	2009-01-09	7.5	CVE 0108 BID MILV SECI OSV
playsms -- playsms	Multiple directory traversal vulnerabilities in playSMS 0.9.3 allow remote attackers to include and execute arbitrary local files via directory traversal sequences in the (1) gateway_module parameter to plugin/gateway/gnokii/init.php and the (2) themes_module parameter to plugin/themes/default/init.php.	2009-01-09	7.5	CVE 5881 BID MILV SECI
playsms -- playsms	Multiple PHP remote file inclusion vulnerabilities in playSMS 0.9.3 allow remote attackers to execute arbitrary PHP code via a URL in the (1) apps_path[plug] parameter to plugin/gateway/gnokii/init.php, the (2) apps_path[themes] parameter to plugin/themes/default/init.php, and the (3) apps_path[libs] parameter to lib/function.php.	2009-01-09	7.5	CVE 0103 BID MILV SECI
proxim -- tsunami_mp.11_2411	The Proxim Wireless Tsunami MP.11 2411 with firmware 3.0.3 has public as its default SNMP read/write community, which makes it easier for remote attackers to obtain sensitive information or modify SNMP variables.	2009-01-07	10.0	CVE 5866 BUG MISC
	SQL injection vulnerability in			

riotpix -- riotpix	index.php in RiotPix 0.61 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter. NOTE: some of these details are obtained from third party information.	2009-01-09	7.5	CVE 0109 BID MILV SECU
riotpix -- riotpix	SQL injection vulnerability in read.php in RiotPix 0.61 and earlier allows remote attackers to execute arbitrary SQL commands via the forumid parameter.	2009-01-09	7.5	CVE 0110 BID MILV SECU
se-ed -- ezpack	SQL injection vulnerability in index.php in EZpack 4.2b2 allows remote attackers to execute arbitrary SQL commands via the qType parameter in a webboard prog action.	2009-01-09	7.5	CVE 0104 BID MILV
sun -- jdk sun -- jre sun -- sdk	Heap-based buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; and SDK and JRE 1.4.2_18 and earlier might allow remote attackers to execute arbitrary code via a crafted TrueType font file.	2009-01-09	9.3	CVE 5356 SUN
sun -- jdk sun -- jre sun -- sdk	Buffer overflow in Java Runtime Environment (JRE) for Sun JDK and JRE 6 Update 10 and earlier; JDK and JRE 5.0 Update 16 and earlier; SDK and JRE 1.4.2_18 and earlier; and SDK and JRE 1.3.1_23 and earlier might allow remote attackers to execute arbitrary code via unknown vectors related to "image processing code."	2009-01-09	9.3	CVE 5359 SUN
v-gn -- userlocator	SQL injection vulnerability in locator.php in the Userlocator module 3.0 for Woltlab Burning Board (wBB) allows remote attackers to execute arbitrary SQL commands via the y parameter in a get_user action.	2009-01-06	7.5	CVE 5863 BID MILV
yerba -- yerba	Yerba SACphp 6.3 and earlier allows remote attackers to bypass authentication and gain administrative access via a galleta [sesion] cookie that has a value	2009-01-08	7.5	CVE 5873 XF BID MILV

	beginning with 1:1: followed by a username.			SECU

Back to top

Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch In**
apple -- safari	Memory leak in WebKit.dll in WebKit, as used by Apple Safari 3.2 on Windows Vista SP1, allows remote attackers to cause a denial of service (memory consumption and browser crash) via a long ALINK attribute in a BODY element in an HTML document.	2009-01-02	5.0	CVE-200 5821 XF BID MISC MISC
checkpoint -- vpn-1	Check Point VPN-1 R55, R65, and other versions, when Port Address Translation (PAT) is used, allows remote attackers to discover intranet IP addresses via a packet with a small TTL, which triggers an ICMP_TIMXCEED_INTRANS (aka ICMP time exceeded in-transit) response containing an encapsulated IP packet with an intranet address, as demonstrated by a TCP packet to the firewall management server on port 18264.	2009-01-06	5.0	CVE-200 5849 MISC CONFIR MISC
chicomas -- chicomas	Chilek Content Management System (aka ChiCoMaS) 2.0.4 and earlier stores sensitive information under the web root with insufficient access control, which allows remote attackers to (1) obtain database credentials via a direct request for config.inc or (2) read database backups via a request for a backup/ URI.	2009-01-06	5.0	CVE-200 5853 BUGTRA MILW0R MISC SECUNI
cisco -- gss_4480_global_site_selector cisco -- gss_4490_global_site_selector cisco -- gss_4491_global_site_selector cisco -- gss_4492r_global_site_selector	dnsserver in Cisco Application Control Engine Global Site Selector (GSS) before 3.0(1) allows remote attackers to cause a denial of service (daemon crash) via a series of crafted DNS requests, aka Bug ID	2009-01-08	5.0	CVE-200 3819 CISCO

	CSCsj70093.			
class -- class	Directory traversal vulnerability in scripts/export.php in ClaSS before 0.8.61 allows remote attackers to read arbitrary files via directory traversal sequences in the ftype parameter. NOTE: some of these details are obtained from third party information.	2009-01-06	5.0	CVE-200 5856 XF BID CONFIR SECUNI OSVDB
constructr -- constructr-cms	SQL injection vulnerability in index.php in Constructr CMS 3.02.5 and earlier, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the show_page parameter.	2009-01-06	5.1	CVE-200 5859 BID MILW0R SECUNI
constructr -- constructr-cms	Directory traversal vulnerability in backend/template.php in Constructr CMS 3.02.5 and earlier, when register_globals is enabled and magic_quotes_gpc is disabled, allows remote attackers to create or read arbitrary files via directory traversal sequences in the edit_file parameter.	2009-01-06	5.1	CVE-200 5860 MILW0R SECUNI
eid -- eidlib	Belgian eID middleware (eidlib) 2.6.0 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0049 MISC
emefa -- emefa_guestbook	Emefa Guestbook 3.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download the database file via a direct request for guestbook.mdb.	2009-01-06	5.0	CVE-200 5852 MILW0R SECUNI

expinion -- poll_pro	Cross-site request forgery (CSRF) vulnerability in admin/agent_edit.asp in PollPro 3.0 allows remote attackers to create or modify accounts as administrators via the username, password, and name parameters.	2009-01-09	6.8	CVE-200 0112 XF SECUNI BUGTR/
faststone -- image_viewer	FastStone Image Viewer 3.6 allows user-assisted attackers to cause a denial of service (application crash) via a malformed BMP image with large width and height values, possibly a related issue to CVE-2007-1942.	2009-01-08	4.3	CVE-200 5870 BUGTR/ MILW0R
freedesktop -- xdg-open	Interaction error in xdg-open allows remote attackers to execute arbitrary code by sending a file with a dangerous MIME type but using a safe type that Firefox sends to xdg-open, which causes xdg-open to process the dangerous file type through automatic type detection, as demonstrated by overwriting the .desktop file.	2009-01-07	6.8	CVE-200 0068 MISC MLIST
freelyrics -- freelyrics	Directory traversal vulnerability in source.php in FreeLyrics 1.0 allows remote attackers to read arbitrary files via directory traversal sequences in the p parameter. NOTE: some of these details are obtained from third party information.	2009-01-06	5.0	CVE-200 5861 BID MILW0R SECUNI
fujitsu-siemens -- webtransactions	Multiple cross-site scripting (XSS) vulnerabilities in Fujitsu-Siemens WebTransactions 7.0, 7.1, and possibly other versions allow remote attackers to inject arbitrary web script or HTML via vectors associated with (1) a demo application shipped with WebTransactions and possibly (2) an unspecified "dynamic application."	2009-01-05	4.3	CVE-200 5842 CONFIR
	Gale 0.99 and earlier does not properly check the return value from the OpenSSL			

gale -- gale	EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0047 MISC
ietf -- md5	The MD5 Message-Digest Algorithm is not collision resistant, which makes it easier for context-dependent attackers to conduct spoofing attacks, as demonstrated by attacks on the use of MD5 in the signature algorithm of an X.509 certificate.	2009-01-05	5.0	CVE-200 2761 CERT-VI MISC MISC MISC BID BUGTRA MISC MISC MISC MISC MISC
isc -- bind	BIND 9.4.3 and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0025 MISC
joomla -- xstandard	Directory traversal vulnerability in attachmentlibrary.php in the XStandard component for Joomla! 1.5.8 and earlier allows remote attackers to list arbitrary directories via a .. (dot dot) in the X_CMS_LIBRARY_PATH HTTP header.	2009-01-09	5.0	CVE-200 0113 BID MILW0R SECUNI
knowledgetree_document_management -- knowledgetree_document_management	The DropDocuments plugin in KnowledgeTree before 3.5.4a allows remote authenticated users to gain administrative privileges via a certain sequence of "browse documents" and dashboard requests.	2009-01-06	6.5	CVE-200 5857 BID SECUNI
	Multiple cross-site scripting (XSS) vulnerabilities in KnowledgeTree before 3.5.4a			CVE-200

knowledgetree_document_management -- knowledgetree_document_management	allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different issue than CVE-2007-4281.	2009-01-06	4.3	5858 BID CONFIR SECUNI
lasso -- lasso	Lasso 2.2.1 and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0050 MISC
microsoft -- money	An ActiveX control in prtstb06.dll in Microsoft Money 2006, when used with WScript in Windows Script Host (WSH) on Windows Vista, allows remote attackers to cause a denial of service (access violation and application crash) via a zero value for the Startup property.	2009-01-02	4.3	CVE-200 5823 XF MISC
microsoft -- internet_explorer	Microsoft Internet Explorer 6.0 through 8.0 beta2 allows remote attackers to cause a denial of service (application crash) via an onload=screen[""] attribute value in a BODY element.	2009-01-08	4.3	CVE-200 0072 XF BID MISC
myphpscripts -- login_session	Multiple cross-site scripting (XSS) vulnerabilities in login.php in myPHPscripts Login Session 2.0 allow remote attackers to inject arbitrary web script or HTML via the (1) ls_user and (2) ls_email parameters (aka the User form) in an ls_register action. NOTE: some of these details are obtained from third party information.	2009-01-06	4.3	CVE-200 5854 XF BID MILW0R SECUNI
myphpscripts -- login_session	myPHPscripts Login Session 2.0 stores sensitive information under the web root with insufficient access control, which allows remote attackers to discover usernames, e-mail addresses, and password hashes	2009-01-06	5.0	CVE-200 5855 XF MILW0R SECUNI

	via a direct request for users.txt.			
nortel -- multimedia_communication_server_5100	Nortel Multimedia Communication Server (MSC) 5100 3.0.13 does not verify credentials during call placement, which allows remote attackers to spoof and redirect VoIP calls, possibly related to the snoop command.	2009-01-08	6.4	CVE-200 5871 XF BID FRSIRT MISC CONFIR SECUNI
ntp -- ntp	NTP 4.2.4 before 4.2.4p5 and 4.2.5 before 4.2.5p150 does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0021 MISC
openevidence -- openevidence	OpenEvidence 1.0.6 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0048 MISC
openssl -- openssl	OpenSSL 0.9.8i and earlier does not properly check the return value from the EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys.	2009-01-07	5.0	CVE-200 5077 MISC
pdfjam -- pdfjam	Multiple untrusted search path vulnerabilities in pdfjam allow local users to gain privileges via a Trojan horse program in (1) the current working directory or (2) /var/tmp, related to the (a) pdf90, (b) pdfjoin, and (c) pdfnup scripts.	2009-01-05	4.6	CVE-200 5843 CONFIR MLIST

phpauctions -- phpauctions	Cross-site scripting (XSS) vulnerability in profile.php in PHPAuctions (aka PHPAuctionSystem) allows remote attackers to inject arbitrary web script or HTML via the user_id parameter.	2009-01-09	4.3	CVE-200 0107 BID SECUNI OSVDB MILW0R
phpclanwebsite -- phpclanwebsite	Multiple SQL injection vulnerabilities in Phpclanwebsite (aka PCW) 1.23.3 Fix Pack 5 and earlier, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the (1) page parameter to index.php, (2) form_id parameter to pcw/processforms.php, (3) pcwlogin and (4) pcw_pass parameters to pcw/setlogin.php, (5) searchvalue parameter to pcw/downloads.php, and the (6) searchvalue and (7) whichfield parameter to pcw/downloads.php, a different vector than CVE-2006-0444.	2009-01-08	6.8	CVE-200 5877 BID MILW0R SECUNI
phpclanwebsite -- phpclanwebsite	Multiple directory traversal vulnerabilities in Phpclanwebsite (aka PCW) 1.23.3 Fix Pack 5 and earlier, when magic_quotes_gpc is disabled and register_globals is enabled, allow remote attackers to include and execute arbitrary files via a .. (dot dot) in the (1) boxname parameter to theme/superchrome/box.php and the (2) theme parameter to phpclanwebsite/footer.php.	2009-01-08	5.1	CVE-200 5878 BID MILW0R SECUNI
phpclanwebsite -- phpclanwebsite	Cross-site scripting (XSS) vulnerability in index.php in Phpclanwebsite (aka PCW) 1.23.3 Fix Pack 5 and earlier, allows remote attackers to inject arbitrary web script or HTML via the page parameter and other unspecified vectors.	2009-01-08	4.3	CVE-200 5879 BID MILW0R SECUNI
	Cross-site scripting (XSS) vulnerability in the Proxim			CVE-200

proxim -- tsunami_mp.11_2411	Wireless Tsunami MP.11 2411 with firmware 3.0.3 allows remote authenticated users to inject arbitrary web script or HTML via the system.sysName.0 SNMP OID.	2009-01-08	4.3	5869 XF BID BUGTR/ MISC
samba -- samba	Samba 3.2.0 through 3.2.6, when registry shares are enabled, allows remote authenticated users to access the root filesystem via a crafted connection request that specifies a blank share name.	2009-01-05	6.3	CVE-200 0022 CONFIR SECUNI
se-ed -- ezpack	Cross-site scripting (XSS) vulnerability in index.php in EZpack 4.2b2 allows remote attackers to inject arbitrary web script or HTML via the mdfd parameter in a prog action.	2009-01-09	4.3	CVE-200 0105 BID MILW0R
sixapart -- movable_type	Multiple cross-site scripting (XSS) vulnerabilities in Six Apart Movable Type (MT) before 4.23 allow remote attackers to inject arbitrary web script or HTML via a (1) MTEntryAuthorUsername, (2) MTAuthorDisplayName, (3) MTEntryAuthorDisplayName, or (4) MTCommenterName field in a Profile View template; a (5) listing screen or (6) edit screen in the CMS app; (7) a TrackBack title, related to the HTML sanitization library; or (8) a user archive name (aka archive title) on a published Community Blog template.	2009-01-05	4.3	CVE-200 5845 CONFIR
sixapart -- movable_type	Six Apart Movable Type (MT) before 4.23 allows remote authenticated users with create permission for posts to bypass intended access restrictions and publish posts via a "system-wide entry listing screen."	2009-01-05	4.0	CVE-200 5846 BID CONFIR
	Sun GridEngine 5.3 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers			CVE-200

sun -- grid_engine	to bypass validation of the certificate chain via a malformed SSL/TLS signature for DSA and ECDSA keys, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	0046 MISC
sun -- opensolaris sun -- solaris	Unspecified vulnerability in the nfs4rename_persistent_fh function in the NFS 4 (aka NFSv4) client in the kernel in Sun Solaris 10 and OpenSolaris before snv_102 allows local users to cause a denial of service (recursive mutex_enter and panic) via unspecified vectors.	2009-01-07	4.9	CVE-200 0069 CONFIR
webcamxp -- webcamxp	Directory traversal vulnerability in webcamXP 5.3.2.375 and 5.3.2.410 build 2132 allows remote attackers to read arbitrary files via a ..%2F (encoded dot dot slash) in the URI.	2009-01-06	5.0	CVE-200 5862 XF BID MILW0R SECUNI
yerba -- yerba	Directory traversal vulnerability in Yerba SACphp 6.3 allows remote attackers to read arbitrary files, and possibly have other impact, via directory traversal sequences in the mod field contained in the base64-encoded SID parameter to an unspecified component. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-01-07	5.0	CVE-200 5867 SECUNI
zxid -- zxid	ZXID 0.29 and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.	2009-01-07	5.0	CVE-200 0051 MISC

Back to top

Low Vulnerabilities				
Primary			**CVSS**	**Source &**

Vendor -- Product	Description	Published	Score	Patch Info
constructr -- constructr-cms	Constructr CMS 3.02.5 and earlier stores passwords in cleartext in a MySQL database, which allows context-dependent attackers to obtain sensitive information by reading the hash column.	2009-01-05	2.6	CVE-2008-5847 MILW0RM
mozilla -- firefox	Mozilla Firefox 3.0.5 and earlier 3.0.x versions, when designMode is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a certain (a) replaceChild or (b) removeChild call, followed by a (1) queryCommandValue, (2) queryCommandState, or (3) queryCommandIndeterm call.	2009-01-08	2.6	CVE-2009-0071 CONFIRM CONFIRM BID FULLDISC FULLDISC FULLDISC

Back to top