Vulnerability Summary for the Week of June 23, 2014

Please Note:

- The vulnerabilities are cattegorized by their level of severity which is either High, Medium or Low.
- The CVE indentity number is the publicly known ID given to that particular vulnerability. Therefore you can search the status of that particular vulnerability using that ID.
- The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- photoshop_cs5	Stack-based buffer overflow in the U3D.8BI library plugin in Adobe Photoshop CS5 12.x before 12.0.5 and CS5.1 12.1.x before 12.1.1 allows remote attackers to execute arbitrary code via a long Collada asset element in a DAE file, as demonstrated by the cameraYFov value in the contributor comments element.	2014-06-19	9.3	CVE-2012-2052
alienvault -- open_source_security_information_management	The av-centerd SOAP service in AlienVault OSSIM before 4.7.0 allows remote attackers to execute arbitrary commands via a crafted (1) update_system_info_debian_package, (2) ossec_task, (3) set_ossim_setup admin_ip, (4) sync_rserver, or (5) set_ossim_setup framework_ip request, a different vulnerability than CVE-2014-3805.	2014-06-13	10.0	CVE-2014-3804
alienvault -- open_source_security_information_management	The av-centerd SOAP service in AlienVault OSSIM before 4.7.0 allows remote attackers to execute arbitrary commands via a crafted (1) get_license, (2) get_log_line, or (3) update_system/upgrade_pro_web request, a	2014-06-13	10.0	CVE-2014-3805

	different vulnerability than CVE-2014-3804.			
alienvault -- open_source_security_information_management	The av-centerd SOAP service in AlienVault OSSIM before 4.8.0 allows remote attackers to create arbitrary files and execute arbitrary code via a crafted set_file request.	2014-06-18	10.0	CVE-2014-4151
alienvault -- open_source_security_information_management	The av-centerd SOAP service in AlienVault OSSIM before 4.8.0 allows remote attackers to execute arbitrary code via a crafted remote_task request, related to injecting an ssh public key.	2014-06-18	10.0	CVE-2014-4152
alienvault -- open_source_security_information_management	The av-centerd SOAP service in AlienVault OSSIM before 4.8.0 allows remote attackers to read arbitrary files via a crafted get_file request.	2014-06-18	7.8	CVE-2014-4153
belkin -- n150_f9k1009	Absolute path traversal vulnerability in the webproc cgi module on the Belkin N150 F9K1009 v1 router with firmware before 1.00.08 allows remote attackers to read arbitrary files via a full pathname in the getpage parameter.	2014-06-19	7.8	CVE-2014-2962
cisco -- asr_9001	Cisco IOS XR 4.1.2 through 5.1.1 on ASR 9000 devices, when a Trident-based line card is used, allows remote attackers to cause a denial of service (NP chip and line card reload) via malformed IPv6 packets, aka Bug ID CSCun71928.	2014-06-14	7.1	CVE-2014-2176
citrix -- access_gateway_plug-in	Heap-based buffer overflow in the StartEpa method in the nsepacom ActiveX control (nsepa.exe) in Citrix Access Gateway Enterprise Edition Plug-in for Windows 9.x before 9.3-57.5 and 10.0 before 10.0-69.4 allows remote attackers to execute arbitrary code via a long CSEC HTTP response header.	2014-06-18	9.3	CVE-2011-2592
hp -- service_virtualization	Directory traversal vulnerability in CommunicationServlet in HP Service Virtualization 3.x before 3.50.1, when the AutoPass license server is enabled, allows remote attackers to create arbitrary files and consequently execute arbitrary code via unspecified vectors, aka ZDI-CAN-2031.	2014-06-18	10.0	CVE-2013-6221

hp -- executive_scorecard	The Java Glassfish Admin Console in HP Executive Scorecard 9.40 and 9.41 does not require authentication, which allows remote attackers to execute arbitrary code via a session on TCP port 10001, aka ZDI-CAN-2116.	2014-06-19	10.0	CVE-2014-2609
hp -- executive_scorecard	Directory traversal vulnerability in the Content Acceleration Pack (CAP) web application in HP Executive Scorecard 9.40 and 9.41 allows remote authenticated users to execute arbitrary code by uploading an executable file, aka ZDI-CAN-2117.	2014-06-19	7.1	CVE-2014-2610
hp -- executive_scorecard	Directory traversal vulnerability in the fndwar web application in HP Executive Scorecard 9.40 and 9.41 allows remote authenticated users to execute arbitrary code, or obtain sensitive information or delete data, via unspecified vectors, aka ZDI-CAN-2120.	2014-06-19	9.0	CVE-2014-2611
huawei -- campus_series_switch_software	Multiple heap-based buffer overflows in Huawei Campus Series Switches S3700HI, S5700, S6700, S3300HI, S5300, S6300, S9300, S7700, and LSW S9700 with software V200R001 before V200R001SPH013; S5700, S6700, S5300, and S6300 with software V200R002 before V200R002SPH005; S7700, S9300, S9300E, S5300, S5700, S6300, S6700, S2350, S2750, and LSW S9700 with software V200R003 before V200R003SPH005; and S7700, S9300, S9300E, and LSW S9700 with software V200R005 before V200R005C00SPC300 allow remote attackers to cause a denial of service (device restart) via a crafted length field in a packet.	2014-06-17	7.8	CVE-2014-4190
jogamp -- joal	Multiple unspecified vulnerabilities in OpenAL32.dll in JOAL 2.0-rc11, as used in JOGAMP, allow context-dependent attackers to execute arbitrary code via a crafted parameter to the (1) alAuxiliaryEffectSlotf1, (2) alBuffer3f1, (3) alBufferfv1, (4) alDeleteEffects1, (5) alEffectf1, (6) alEffectfv1, (7) alEffectiv1, (8) alEnable1, (9) alFilterfv1, (10) alFilteriv1, (11) alGenAuxiliaryEffectSlots1, (12) alGenEffects1,	2014-06-13	10.0	CVE-2013-4099

	(13) alGenFilters1, (14) alGenSources1, (15) alGetAuxiliaryEffectSlotiv1, (16) alGetBuffer3f1, (17) alGetBuffer3i1, (18) alGetBufferf1, (19) alGetBufferiv1, (20) alGetDoublev1, (21) alGetEffectf1, (22) alGetEffectfv1, (23) alGetEffectiv1, (24) alGetEnumValue1, (25) alGetFilteri1, (26) alGetFilteriv1, (27) alGetFloat1, (28) alGetFloatv1, (29) alGetListener3f1, (30) alGetListener3i1, (31) alGetListenerf1, (32) alGetListeneri1, (33) alGetListeneriv1, (34) alGetProcAddress1, (35) alGetProcAddressStatic, (36) alGetSource3f1, (37) alGetSource3i1, (38) alGetSourcef1, (39) alGetSourcefv1, (40) alGetSourcei1, (41) alGetSourceiv1, (42) alGetString1java/lang/String;, (43) alIsAuxiliaryEffectSlot1, (44) alIsBuffer1, (45) alIsEffect1, (46) alIsExtensionPresent1, (47) alIsFilter1, (48) alListener3f1, (49) alListener3i1, (50) alListenerf1, (51) alListenerfv1, (52) alListeneri1, (53) alListeneriv1, (54) alSource3f1, (55) alSource3i1, (56) alSourcef1, (57) alSourcefv1, (58) alSourcei1, (59) alSourceiv1, (60) alSourcePause1, (61) alSourcePausev1, (62) alSourcePlay1, (63) alSourcePlayv1, (64) alSourceQueueBuffers1, (65) alSourceRewindv1, (66) alSourceStop1, (67) alSourceStopv1, (68) alSourceUnqueueBuffers1, or (69) alSpeedOfSound1 method in jogamp.openal.ALImpl.dispatch.			
juniper -- netscreen-5200	Unspecified vulnerability in the Juniper Networks NetScreen Firewall products with ScreenOS before 6.3r17, when configured to use the internal DNS lookup client, allows remote attackers to cause a denial of service (crash and reboot) via vectors related to a DNS lookup.	2014-06-13	7.8	CVE-2014-3813
juniper -- netscreen-5200	The Juniper Networks NetScreen Firewall devices with ScreenOS before 6.3r17, when configured to use the internal DNS lookup client, allows remote attackers to cause a denial of service	2014-06-13	7.8	CVE-2014-3814

	(crash and reboot) via a sequence of malformed packets to the device IP.			
justsystems -- ichitaro	JustSystems JUST Online Update, as used in Ichitaro through 2014 and other products, does not properly validate signatures of update modules, which allows remote attackers to spoof modules and execute arbitrary code via a crafted signature.	2014-06-16	7.6	CVE-2014-2003
microsoft -- internet_explorer	Microsoft Internet Explorer 9 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-19	9.3	CVE-2014-2782
nice -- recording_express	Multiple SQL injection vulnerabilities in NICE Recording eXpress (aka Cybertech eXpress) 6.5.7 and earlier allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	2014-06-18	7.5	CVE-2014-4305
novell -- open_enterprise_server	Directory traversal vulnerability in iPrint in Novell Open Enterprise Server (OES) 11 SP1 before Maintenance Update 9151 on Linux has unspecified impact and remote attack vectors.	2014-06-18	10.0	CVE-2014-0598
senkas -- kolibri	Stack-based buffer overflow in Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a HEAD request.	2014-06-13	7.5	CVE-2010-5301
senkas -- kolibri	Stack-based buffer overflow in Kolibri 2.0 allows remote attackers to execute arbitrary code via a long URI in a GET request.	2014-06-13	7.5	CVE-2014-4158
symantec -- web_gateway	SNMPConfig.php in the management console in Symantec Web Gateway (SWG) before 5.2.1 allows remote attackers to execute arbitrary commands via unspecified vectors.	2014-06-18	7.9	CVE-2013-5017
ubi -- rayman_legends	Stack-based buffer overflow in Ubisoft Rayman	2014-06-19	7.5	CVE-2014-4334

	Legends before 1.3.140380 allows remote attackers to execute arbitrary code via a long string in the "second connection" to TCP port 1001.			
webtitan -- webtitan	SQL injection vulnerability in categories-x.php in WebTitan before 4.04 allows remote attackers to execute arbitrary SQL commands via the sortkey parameter.	2014-06-18	7.5	CVE-2014-4307
wireshark -- wireshark	wiretap/libpcap.c in the libpcap file parser in Wireshark 1.10.x before 1.10.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted packet-trace file that includes a large packet.	2014-06-18	9.3	CVE-2014-4174

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
ajenti -- ajenti	Multiple cross-site scripting (XSS) vulnerabilities in the respond_error function in routing.py in Eugene Pankov Ajenti before 1.2.21.7 allow remote attackers to inject arbitrary web script or HTML via the PATH_INFO to (1) resources.js or (2) resources.css in ajenti:static/, related to the traceback page.	2014-06-18	4.3	CVE-2014-4301
algosec -- fireflow	Cross-site scripting (XSS) vulnerability in AlgoSec FireFlow 6.3-b230 allows remote attackers to inject arbitrary web script or HTML via a user signature to SelfService/Prefs.html.	2014-06-16	4.3	CVE-2014-4164

apache -- myfaces	Multiple directory traversal vulnerabilities in MyFaces JavaServer Faces (JSF) in Apache MyFaces Core 2.0.x before 2.0.12 and 2.1.x before 2.1.6 allow remote attackers to read arbitrary files via a .. (dot dot) in the (1) ln parameter to faces/javax.faces.resource/web.xml or (2) the PATH_INFO to faces/javax.faces.resource/.	2014-06-19	5.0	CVE-2011-4367
apache -- open_for_business_project	Multiple cross-site scripting (XSS) vulnerabilities in Apache Open For Business Project (aka OFBiz) 10.04.x before 10.04.02 allow remote attackers to inject arbitrary web script or HTML via (1) a parameter array in freemarker templates, the (2) contentId or (3) mapKey parameter in a cms event request, which are not properly handled in an error message, or unspecified input in (4) an ajax request to the getServerError function in checkoutProcess.js or (5) a Webslinger component request. NOTE: some of these details are obtained from third party information.	2014-06-19	4.3	CVE-2012-1621
arris -- sbg901	Multiple cross-site request forgery (CSRF) vulnerabilities in goform/RgDdns in ARRIS (formerly Motorola) SBG901 SURFboard Wireless Cable Modem allow remote attackers to hijack the authentication of administrators for requests that (1) change the dns service via the DdnsService parameter, (2) change the username via the DdnsUserName parameter, (3) change the password via the DdnsPassword parameter, or (4) change the host name via the DdnsHostName parameter.	2014-06-19	6.8	CVE-2014-3778
axigen -- axigen_mail_server	Cross-site scripting (XSS) vulnerability in Axigen Mail Server 8.0.1 allows remote attackers to inject arbitrary web script or HTML via the body of an email.	2014-06-18	4.3	CVE-2012-2592
barracudadrive -- barracudadrive	Multiple cross-site scripting (XSS) vulnerabilities in BarracudaDrive 6.7.2 allow remote attackers to inject arbitrary web script or HTML via the (1) host or (2) password parameter to rtl/protected/admin/ddns/.	2014-06-19	4.3	CVE-2014-4335

boonex -- dolphin	SQL injection vulnerability in administration/profiles.php in BoonEx Dolphin 7.1.4 and earlier allows remote authenticated administrators to execute arbitrary SQL commands via the members[] parameter. NOTE: this can be exploited by remote attackers by leveraging CVE-2014-4333.	2014-06-19	6.5	CVE-2014-3810
boonex -- dolphin	Cross-site request forgery (CSRF) vulnerability in administration/profiles.php in Dolphin 7.1.4 and earlier allows remote attackers to hijack the authentication of administrators for requests that conduct SQL injection attacks via the members[] parameter, related to CVE-2014-3810.	2014-06-19	6.8	CVE-2014-4333
c-board_moyuku_project -- c-board_moyuku	Cross-site scripting (XSS) vulnerability in C-BOARD Moyuku 1.01b6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-14	4.3	CVE-2014-2002
canonical -- ubuntu_linux	The OpenStack Nova (python-nova) package 1:2013.2.3-0 before 1:2013.2.3-0ubuntu1.2 and 1:2014.1-0 before 1:2014.1-0ubuntu1.2 and Openstack Cinder (python-cinder) package 1:2013.2.3-0 before 1:2013.2.3-0ubuntu1.1 and 1:2014.1-0 before 1:2014.1-0ubuntu1.1 for Ubuntu 13.10 and 14.04 LTS does not properly set the sudo configuration, which makes it easier for attackers to gain privileges by leveraging another vulnerability.	2014-06-19	5.0	CVE-2013-1068
cisco -- adaptive_security_appliance_software	The WebVPN portal in Cisco Adaptive Security Appliance (ASA) Software 8.4(.7.15) and earlier allows remote authenticated users to obtain sensitive information via a crafted JavaScript file, aka Bug ID CSCui04520.	2014-06-18	4.0	CVE-2014-2151
cisco -- ios_xe	The mDNS implementation in Cisco IOS XE 3.12S does not properly interact with autonomic networking, which allows remote attackers to obtain sensitive networking-services information by sniffing the network or overwrite networking-services data via a crafted mDNS response, aka Bug ID CSCun64867.	2014-06-14	4.8	CVE-2014-3290

cisco -- nx-os	The HSRP implementation in Cisco NX-OS 6.2(2a) and earlier allows remote attackers to bypass authentication and cause a denial of service (group-member state modification and traffic blackholing) via malformed HSRP packets, aka Bug ID CSCup11309.	2014-06-14	4.8	CVE-2014-3295
clip-bucket -- clipbucket	Cross-site scripting (XSS) vulnerability in signup.php in ClipBucket allows remote attackers to inject arbitrary web script or HTML via the Username field.	2014-06-17	4.3	CVE-2014-4187
debian -- apt	APT before 1.0.4 does not properly validate source packages, which allows man-in-the-middle attackers to download and install Trojan horse packages by removing the Release signature.	2014-06-17	4.0	CVE-2014-0478
digium -- asterisk	The Publish/Subscribe Framework in the PJSIP channel driver in Asterisk Open Source 12.x before 12.3.1, when sub_min_expiry is set to zero, allows remote attackers to cause a denial of service (assertion failure and crash) via an unsubscribe request when not subscribed to the device.	2014-06-17	4.3	CVE-2014-4045
digium -- asterisk	Asterisk Open Source 11.x before 11.10.1 and 12.x before 12.3.1 and Certified Asterisk 11.6 before 11.6-cert3 allows remote authenticated Manager users to execute arbitrary shell commands via a MixMonitor action.	2014-06-17	6.5	CVE-2014-4046
digium -- asterisk	Asterisk Open Source 1.8.x before 1.8.28.1, 11.x before 11.10.1, and 12.x before 12.3.1 and Certified Asterisk 1.8.15 before 1.8.15-cert6 and 11.6 before 11.6-cert3 allows remote attackers to cause a denial of service (connection consumption) via a large number of (1) inactive or (2) incomplete HTTP connections.	2014-06-17	5.0	CVE-2014-4047
digium -- asterisk	The PJSIP Channel Driver in Asterisk Open Source before 12.3.1 allows remote attackers to cause a denial of service (deadlock) by terminating a subscription request before it is complete, which triggers a SIP transaction timeout.	2014-06-17	4.3	CVE-2014-4048
echoping_project --	Multiple buffer overflows in readline.c in Echoping	2014-06-16	6.8	CVE-2010-5111

echoping	6.0.2 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted reply in the (1) TLS_readline or (2) SSL_readline function, related to the EchoPingHttps Smokeping probe.			
emc -- rsa_bsafe_toolkits	The default configuration of EMC RSA BSAFE Toolkits and RSA Data Protection Manager (DPM) 20130918 uses the Dual Elliptic Curve Deterministic Random Bit Generation (Dual_EC_DRBG) algorithm, which makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms by leveraging unspecified "security concerns," aka the ESA-2013-068 issue. NOTE: this issue has been SPLIT from CVE-2007-6755 because the vendor announcement did not state a specific technical rationale for a change in the algorithm; thus, CVE cannot reach a conclusion that a CVE-2007-6755 concern was the reason, or one of the reasons, for this change.	2014-06-17	5.8	CVE-2013-6078
emc -- rsa_bsafe-c_toolkits	The TLS implementation in EMC RSA BSAFE-C Toolkits (aka Share for C and C++) sends a long series of random bytes during use of the Dual_EC_DRBG algorithm, which makes it easier for remote attackers to obtain plaintext from TLS sessions by recovering the algorithm's inner state, a different issue than CVE-2007-6755.	2014-06-17	5.0	CVE-2014-4191
emc -- rsa_bsafe-c_toolkits	The Dual_EC_DRBG implementation in EMC RSA BSAFE-C Toolkits (aka Share for C and C++) processes certain requests for output bytes by considering only the requested byte count and not the use of cached bytes, which makes it easier for remote attackers to obtain plaintext from TLS sessions by recovering the algorithm's inner state, a different issue than CVE-2007-6755.	2014-06-17	5.0	CVE-2014-4192
emc -- rsa_bsafe-java_toolkits	The TLS implementation in EMC RSA BSAFE-Java Toolkits (aka Share for Java) supports the Extended Random extension during use of the Dual_EC_DRBG algorithm, which makes it easier for remote attackers to obtain plaintext from TLS	2014-06-17	5.0	CVE-2014-4193

	sessions by requesting long nonces from a server, a different issue than CVE-2007-6755.			
f5 -- arx_data_manager	SQL injection vulnerability in the web service in F5 ARX Data Manager 3.0.0 through 3.1.0 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.	2014-06-18	6.5	CVE-2014-2949
featured_comments_plugin_project -- featured_comments	Multiple cross-site request forgery (CSRF) vulnerabilities in the Featured Comments plugin 1.2.1 for WordPress allow remote attackers to hijack the authentication of administrators for requests that change the (1) buried or (2) featured status of a comment via a request to wp-admin/admin-ajax.php.	2014-06-16	6.8	CVE-2014-4163
ham3d -- ham3d_shop_engine	Cross-site scripting (XSS) vulnerability in rating/rating.php in HAM3D Shop Engine allows remote attackers to inject arbitrary web script or HTML via the ID parameter.	2014-06-18	4.3	CVE-2014-4302
hitachi -- jp1/performance_management-manager_web_option	Cross-site request forgery (CSRF) vulnerability in Hitachi Tuning Manager before 7.6.1-06 and 8.x before 8.0.0-04 and JP1/Performance Management - Manager Web Option 07-00 through 07-54 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2014-06-17	6.8	CVE-2014-4188
hitachi -- jp1/performance_management-manager_web_option	Cross-site scripting (XSS) vulnerability in Hitachi Tuning Manager before 7.6.1-06 and 8.x before 8.0.0-04 and JP1/Performance Management - Manager Web Option 07-00 through 07-54 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-17	4.3	CVE-2014-4189
ibm -- pureapplication_system	IBM PureApplication System 1.0 before 1.0.0.4 cfix8 and 1.1 before 1.1.0.4 IF1 allows remote authenticated users to bypass intended access restrictions by establishing an SSH session from a deployed virtual machine.	2014-06-14	6.6	CVE-2014-0960
iij -- seil/b1	The PPP Access Concentrator (PPPAC) on SEIL SEIL/x86 routers 1.00 through 3.10, SEIL/X1 routers 1.00 through 4.50, SEIL/X2 routers 1.00 through 4.50, SEIL/B1 routers 1.00 through 4.50, SEIL/Turbo	2014-06-16	5.0	CVE-2014-2004

	routers 1.80 through 2.17, and SEIL/neu 2FE Plus routers 1.80 through 2.17 allows remote attackers to cause a denial of service (session termination or concentrator outage) via a crafted TCP packet.			
isc -- bind	libdns in ISC BIND 9.10.0 before P2 does not properly handle EDNS options, which allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted packet, as demonstrated by an attack against named, dig, or delv.	2014-06-13	5.0	CVE-2014-3859
jreast -- jr_east_japan	The East Japan Railway Company JR East Japan application before 1.2.0 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to obtain sensitive information via a crafted certificate.	2014-06-19	5.8	CVE-2014-2001
juniper -- fips_infranet_controller_6500	The Juniper Junos Pulse Secure Access Service (SSL VPN) devices with IVE OS before 7.4r5 and 8.x before 8.0r1 and Junos Pulse Access Control Service (UAC) before 4.4r5 and 5.x before 5.0r1 enable cipher suites with weak encryption algorithms, which make it easier for remote attackers to obtain sensitive information by sniffing the network.	2014-06-13	5.0	CVE-2014-3812
microsoft -- malware_protection_engine	mpengine.dll in Microsoft Malware Protection Engine before 1.1.10701.0 allows remote attackers to cause a denial of service (system hang) via a crafted file.	2014-06-18	4.3	CVE-2014-2779
mindreantre -- threewp_email_reflector	Cross-site scripting (XSS) vulnerability in the ThreeWP Email Reflector plugin before 1.16 for WordPress allows remote attackers to inject arbitrary web script or HTML via the Subject of an email.	2014-06-19	4.3	CVE-2012-2572
nice -- recording_express	Multiple cross-site scripting (XSS) vulnerabilities in NICE Recording eXpress (aka Cybertech eXpress) before 6.5.5 allow remote attackers to inject arbitrary web script or HTML via the (1) USRLNM parameter to myaccount/mysettings.edit.validate.asp or the frame parameter to (2)	2014-06-18	4.3	CVE-2014-4308

	iframe.picker.statchannels.asp, (3) iframe.picker.channelgroups.asp, (4) iframe.picker.extensions.asp, (5) iframe.picker.licenseusergroups.asp, (6) iframe.picker.licenseusers.asp, (7) iframe.picker.lookup.asp, or (8) iframe.picker.marks.asp in _ifr/.			
novell -- open_enterprise_server	Cross-site scripting (XSS) vulnerability in iPrint in Novell Open Enterprise Server (OES) 11 SP1 before Maintenance Update 9151 on Linux allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-18	4.3	CVE-2014-0599
ntop -- ntop	Cross-site scripting (XSS) vulnerability in ntop allows remote attackers to inject arbitrary web script or HTML via the title parameter in a list action to plugins/rrdPlugin.	2014-06-16	4.3	CVE-2014-4165
ntop -- ntopng	Cross-site scripting (XSS) vulnerability in lua/host_details.lua in ntopng 1.1 allows remote attackers to inject arbitrary web script or HTML via the host parameter.	2014-06-19	4.3	CVE-2014-4329
openafs -- openafs	OpenAFS 1.6.8 does not properly clear the fields in the host structure, which allows remote attackers to cause a denial of service (uninitialized memory access and crash) via unspecified vectors related to TMAY requests.	2014-06-17	5.0	CVE-2014-4044
openfiler -- openfiler	Multiple cross-site scripting (XSS) vulnerabilities in Openfiler 2.99 allow remote attackers to inject arbitrary web script or HTML via the (1) TinkerAjax parameter to uptime.html, or remote authenticated users to inject arbitrary web script or HTML via the (2) MaxInstances, (3) PassivePorts, (4) Port, (5) ServerName, (6) TimeoutLogin, (7) TimeoutNoTransfer, or (8) TimeoutStalled parameter to admin/services_ftp.html; the (9) dns1 or (10) dns2 parameter to admin/system.html; the (11) newTgtName parameter to admin/volumes_iscsi_targets.html; the User-Agent HTTP header to (12) language.html, (13) login.html,	2014-06-18	4.3	CVE-2014-4309

	or (14) password.html in account/; or the User-Agent HTTP header to (15) account_groups.html, (16) account_users.html, (17) services.html, (18) services_ftp.html, (19) services_iscsi_target.html, (20) services_rsync.html, (21) system_clock.html, (22) system_info.html, (23) system_ups.html, (24) volumes_editpartitions.html, or (25) volumes_iscsi_targets.html in admin/.			
openstack -- keystone	OpenStack Identity (Keystone) before 2013.2.4, 2014.1 before 2014.1.2, and Juno before Juno-2 does not properly handle chained delegation, which allows remote authenticated users to gain privileges by leveraging a (1) trust or (2) OAuth token with impersonation enabled to create a new token with additional roles.	2014-06-17	6.0	CVE-2014-3476
php -- php	Heap-based buffer overflow in the php_parserr function in ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote servers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DNS TXT record, related to the dns_get_record function.	2014-06-18	5.1	CVE-2014-4049
powerpc-utils_project -- powerpc-utils	snap in powerpc-utils 1.2.20 produces an archive with fstab and yaboot.conf files potentially containing cleartext passwords, and lacks a warning about reviewing this archive to detect included passwords, which might allow remote attackers to obtain sensitive information by leveraging access to a technical-support data stream.	2014-06-17	5.0	CVE-2014-4040
ppc64-diag_project -- ppc64-diag	ppc64-diag 2.6.1 allows local users to overwrite arbitrary files via a symlink attack related to (1) rtas_errd/diag_support.c and /tmp/get_dt_files, (2) scripts/ppc64_diag_mkrsrc and /tmp/diagSEsnap/snapH.tar.gz, or (3) lpd/test/lpd_ela_test.sh and /var/tmp/ras.	2014-06-17	4.4	CVE-2014-4038
puppetlabs -- puppet	Puppet Enterprise 2.8.x before 2.8.7 allows remote attackers to obtain sensitive information via vectors involving hiding and unhiding nodes.	2014-06-17	5.0	CVE-2014-3249
redhat --	A certain tomcat7 package for Apache Tomcat 7 in	2014-06-14	5.0	CVE-2014-0186

enterprise_linux	Red Hat Enterprise Linux (RHEL) 7 allows remote attackers to cause a denial of service (CPU consumption) via a crafted request. NOTE: this vulnerability exists because of an unspecified regression.			
reviewboard -- djblets	Cross-site scripting (XSS) vulnerability in util/templatetags/djblets_js.py in Djblets before 0.7.30 and 0.8.x before 0.8.3 for Django, as used in Review Board, allows remote attackers to inject arbitrary web script or HTML via a JSON object, as demonstrated by the name field when changing a user name.	2014-06-16	4.3	CVE-2014-3994
reviewboard -- djblets	Cross-site scripting (XSS) vulnerability in gravatars/templatetags/gravatars.py in Djblets before 0.7.30 and 0.8.x before 0.8.3 for Django allows remote attackers to inject arbitrary web script or HTML via a user display name.	2014-06-16	4.3	CVE-2014-3995
sap -- supplier_relationship_management	Open redirect vulnerability in SAP Supplier Relationship Management (SRM) allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the url parameter.	2014-06-13	5.8	CVE-2014-4159
sap -- netweaver_business_client	Multiple cross-site scripting (XSS) vulnerabilities in the testcanvas node in SAP NetWeaver Business Client (NWBC) allow remote attackers to inject arbitrary web script or HTML via the (1) title or (2) sap-accessibility parameter.	2014-06-13	4.3	CVE-2014-4160
sap -- supplier_relationship_management	Cross-site scripting (XSS) vulnerability in la/umTestSSO.jsp in SAP Supplier Relationship Management (SRM) allows remote attackers to inject arbitrary web script or HTML via the url parameter.	2014-06-13	4.3	CVE-2014-4161
shoutcast -- dnas	Cross-site scripting (XSS) vulnerability in the song history in SHOUTcast DNAS 2.2.1 allows remote attackers to inject arbitrary web script or HTML via the mp3 title field.	2014-06-16	4.3	CVE-2014-4166
sqlbuddy -- sql_buddy	Cross-site scripting (XSS) vulnerability in browse.php in SQL Buddy 1.3.3 and earlier allows	2014-06-18	4.3	CVE-2014-4304

	remote attackers to inject arbitrary web script or HTML via the table parameter.			
symantec -- web_gateway	SQL injection vulnerability in user.php in the management console in Symantec Web Gateway (SWG) before 5.2.1 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors.	2014-06-18	5.2	CVE-2014-1650
symantec -- web_gateway	SQL injection vulnerability in clientreport.php in the management console in Symantec Web Gateway (SWG) before 5.2 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2014-06-18	5.8	CVE-2014-1651
synametrics -- xeams	Cross-site scripting (XSS) vulnerability in Synametrics Technologies Xeams 4.4 Build 5720 allows remote attackers to inject arbitrary web script or HTML via the body of an email.	2014-06-19	4.3	CVE-2012-2569
ulli_horlacher -- fex	Multiple cross-site scripting (XSS) vulnerabilities in Frams' Fast File EXchange (F*EX, aka fex) before fex-20140530 allow remote attackers to inject arbitrary web script or HTML via the (1) akey parameter to rup or (2) disclaimer or (3) gm parameter to fuc.	2014-06-18	4.3	CVE-2014-3876
ulli_horlacher -- fex	Incomplete blacklist vulnerability in Frams' Fast File EXchange (F*EX, aka fex) before fex-20140530 allows remote attackers to conduct cross-site scripting (XSS) attacks via the addto parameter to fup.	2014-06-18	4.3	CVE-2014-3877
webtitan -- webtitan	Directory traversal vulnerability in logs-x.php in WebTitan before 4.04 allows remote attackers to read arbitrary files via a .. (dot dot) in the logfile parameter in a download action.	2014-06-18	5.0	CVE-2014-4306
wireshark -- wireshark	The dissect_frame function in epan/dissectors/packet-frame.c in the frame metadissector in Wireshark 1.10.x before 1.10.8 interprets a negative integer as a length value even though it was intended to represent an error condition, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	2014-06-18	4.3	CVE-2014-4020

yealink -- voip_phone	Cross-site scripting (XSS) vulnerability in Yealink VoIP Phones with firmware 28.72.0.2 allows remote attackers to inject arbitrary web script or HTML via the model parameter to servlet.	2014-06-16	4.3	CVE-2014-3428
zte -- zxv10_w300	Cross-site request forgery (CSRF) vulnerability in the ZTE ZXV10 W300 router with firmware W300V1.0.0a_ZRD_LK allows remote attackers to hijack the authentication of administrators for requests that change the admin password via a request to Forms/tools_admin_1.	2014-06-19	6.8	CVE-2014-4155
zyxel -- p-660hw	Multiple cross-site request forgery (CSRF) vulnerabilities in the Zyxel P-660HW-T1 (v3) wireless router allow remote attackers to hijack the authentication of administrators for requests that change the (1) wifi password or (2) SSID via a request to Forms/WLAN_General_1.	2014-06-16	6.8	CVE-2014-4162

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
drupac -- touch	Multiple cross-site scripting (XSS) vulnerabilities in the Touch theme 7.x-1.x before 7.x-1.9 for Drupal allow remote authenticated users with the Administer themes permission to inject arbitrary web script or HTML via vectors related to the (1) Twitter and (2) Facebook username settings.	2014-06-18	2.1	CVE-2014-4303
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in IBM WebSphere Portal 6.1.0.0 through 6.1.0.6 CF27, 6.1.5.0 through 6.1.5.3 CF27, and 7.0.0 through	2014-06-18	3.5	CVE-2014-0910

	7.0.0.2 CF28 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.			
ibm -- curam_social_program_management	Multiple CRLF injection vulnerabilities in IBM Curam Social Program Management 5.2 SP1 through 6.0.5.4 allow remote authenticated users to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified parameters to custom JSPs.	2014-06-18	3.5	CVE-2014-3012
ibm -- curam_social_program_management	Multiple cross-site scripting (XSS) vulnerabilities in IBM Curam Social Program Management 4.5 SP10 through 6.0.5.4 allow remote authenticated users to inject arbitrary web script or HTML via crafted input to a (1) custom JSP or (2) custom renderer.	2014-06-18	3.5	CVE-2014-3013
ntt -- 050_plus	The NTT 050 plus application before 4.2.1 for Android allows attackers to obtain sensitive information by leveraging the ability to read system log files.	2014-06-18	2.6	CVE-2014-2000
ppc64-diag_project -- ppc64-diag	ppc64-diag 2.6.1 uses 0775 permissions for /tmp/diagSEsnap and does not properly restrict permissions for /tmp/diagSEsnap/snapH.tar.gz, which allows local users to obtain sensitive information by reading files in this archive, as demonstrated by /var/log/messages and /etc/yaboot.conf.	2014-06-17	2.1	CVE-2014-4039
symantec -- web_gateway	Multiple cross-site scripting (XSS) vulnerabilities in the management console in Symantec Web Gateway (SWG) before 5.2 allow remote authenticated users to inject arbitrary web script or HTML via unspecified report parameters.	2014-06-18	2.9	CVE-2014-1652
xen -- xen	Xen 3.2.x through 4.4.x does not properly clean memory pages recovered from guests, which allows local guest OS users to obtain sensitive information via unspecified vectors.	2014-06-18	2.7	CVE-2014-4021

- Sources: http://nvd.nist.gov (For more information visit the National Vulnerabilities Database (NVD) which contains a database of every vulnerability that has ever been published).

Uganda Communications Commission – UGCERT
Email: info@ug-cert.ug Tel + 256 414 302 100/150 **Toll Free:** 0800 133 911
Website www.ug-cert.ug Face book / Twitter: UGCERT