Vulnerability Summary for the Week of May 19, 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**
call-cc -- chicken	Buffer overflow in the "read-u8vector!" procedure in the srfi-4 unit in CHICKEN stable 4.8.0.7 and development snapshots before 4.9.1 allows remote attackers to cause a denial of service (memory corruption and application crash) and possibly execute arbitrary code via a "#f" value in the NUM argument.	2014-05-20	7.5	CVE-2014-3776
canonical -- ltsp_display_manager	The default keybindings for wwm in LTSP Display Manager (ldm) 2.2.x before 2.2.7 allows remote attackers to execute arbitrary commands via the KP_RETURN keybinding, which launches a terminal window.	2014-05-21	10.0	CVE-2012-1166
cogentdatahub -- cogent_datahub	Heap-based buffer overflow in the Web Server in Cogent Real-Time Systems Cogent DataHub before 7.3.5 allows remote attackers to execute arbitrary code via a negative value in the Content-Length field in a request.	2014-05-22	7.5	CVE-2014-3788
cogentdatahub -- cogent_datahub	GetPermissions.asp in Cogent Real-Time Systems Cogent DataHub before 7.3.5 allows remote	2014-05-22	7.5	CVE-2014-3789

	attackers to execute arbitrary commands via unspecified vectors.			
construtiva -- cis_manager_cms	SQL injection vulnerability in Construtiva CIS Manager allows remote attackers to execute arbitrary SQL commands via the email parameter to autenticar/lembrarlogin.asp.	2014-05-20	7.5	CVE-2014-3749
controlsystemworks -- csworks	SQL injection vulnerability in the LiveData service in CSWorks before 2.5.5233.0 allows remote attackers to execute arbitrary SQL commands via vectors related to pathnames contained in web API requests.	2014-05-20	7.5	CVE-2014-2351
efssoft -- easy_file_sharing_web_server	Stack-based buffer overflow in Easy File Sharing (EFS) Web Server 6.8 allows remote attackers to execute arbitrary code via a long string in a cookie UserID parameter to vfolder.ghp.	2014-05-20	10.0	CVE-2014-3791
emerson -- deltav	Emerson DeltaV 10.3.1, 11.3, 11.3.1, and 12.3 uses hardcoded credentials for diagnostic services, which allows remote attackers to bypass intended access restrictions via a TCP session, as demonstrated by a session that uses the telnet program.	2014-05-22	7.5	CVE-2014-2350
google -- chrome	Use-after-free vulnerability in the StyleElement::removedFromDocument function in core/dom/StyleElement.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that triggers tree mutation.	2014-05-21	7.5	CVE-2014-1743
google -- chrome	Integer overflow in the AudioInputRendererHost::OnCreateStream function in content/browser/renderer_host/media/audio_input_renderer_host.cc in Google Chrome before 35.0.1916.114 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large shared-memory allocation.	2014-05-21	7.5	CVE-2014-1744

google -- chrome	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger removal of an SVGFontFaceElement object, related to core/svg/SVGFontFaceElement.cpp.	2014-05-21	7.5	CVE-2014-1745
google -- chrome	Multiple unspecified vulnerabilities in Google Chrome before 35.0.1916.114 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	2014-05-21	7.5	CVE-2014-1749
google -- chrome	Integer underflow in the LCodeGen::PrepareKeyedOperand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.	2014-05-21	7.5	CVE-2014-3152
hanon -- faceid	Hanvon FaceID before 1.007.110 does not require authentication, which allows remote attackers to modify access-control and attendance-tracking data via API commands.	2014-05-22	10.0	CVE-2014-2938
ibm -- websphere_portal	IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0 through 7.0.0.2 CF28, and 8.0 before 8.0.0.1 CF12 does not validate JSP includes, which allows remote attackers to obtain sensitive information, bypass intended request-dispatcher access restrictions, or cause a denial of service (memory consumption) via a crafted URL.	2014-05-22	7.5	CVE-2014-0954
juniper -- network_and_security_manager_software	Unspecified vulnerability in the NSM XDB service in NSM before 2012.2R8 allows remote attackers to execute arbitrary code via unspecified vectors.	2014-05-19	10.0	CVE-2014-3411
juniper -- junos_space	Unspecified vulnerability in Juniper Junos Space before 13.3R1.8, when the firewall in disabled, allows remote attackers to execute arbitrary	2014-05-20	10.0	CVE-2014-3412

	commands via unspecified vectors.			
libgadu -- libgadu	libgadu before 1.11.4 and 1.12.0 before 1.12.0-rc3, as used in Pidgin and other products, allows remote Gadu-Gadu file relay servers to cause a denial of service (memory overwrite) or possibly execute arbitrary code via a crafted message.	2014-05-22	7.5	CVE-2014-3775
microp_project -- microp	Stack-based buffer overflow in MicroP 0.1.1.1600 allows remote attackers to execute arbitrary code via a crafted .mppl file. NOTE: it has been reported that the overflow is in the lpFileName parameter of the CreateFileA function, but the overflow is probably caused by a separate, unnamed function.	2014-05-22	7.5	CVE-2010-5299
microsoft -- internet_explorer	Use-after-free vulnerability in Microsoft Internet Explorer 8 allows remote attackers to execute arbitrary code via crafted JavaScript code that interacts improperly with a CollectGarbage function call on a CMarkup object allocated by the CMarkup::CreateInitialMarkup function.	2014-05-22	9.3	CVE-2014-1770
openvas -- openvas_manager	OpenVAS Manager 3.0 before 3.0.7 and 4.0 before 4.0.4 allows remote attackers to bypass the OMP authentication restrictions and execute OMP commands via a crafted OMP request for version information, which causes the state to be set to CLIENT_AUTHENTIC, as demonstrated by the omp_xml_handle_end_element function in omp.c.	2014-05-19	7.5	CVE-2013-6765
openvas -- openvas_administrator	OpenVAS Administrator 1.2 before 1.2.2 and 1.3 before 1.3.2 allows remote attackers to bypass the OAP authentication restrictions and execute OAP commands via a crafted OAP request for version information, which causes the state to be set to CLIENT_AUTHENTIC.	2014-05-19	7.5	CVE-2013-6766
realnetworks -- realplayer	The GetGUID function in codecs/dmp4.dll in RealNetworks RealPlayer 16.0.3.51 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (write access violation and application crash) via a	2014-05-20	9.3	CVE-2014-3444

	malformed .3gp file.			
skyboxsecurity -- skybox_view_appliance_iso	Skybox View Appliances with ISO 6.3.33-2.14, 6.3.31-2.14, 6.4.42-2.54, 6.4.45-2.56, and 6.4.46-2.57 does not properly restrict access to the Admin interface, which allows remote attackers to obtain sensitive information via a request to (1) scripts/commands/getSystemInformation or (2) scripts/commands/getNetworkConfigurationInfo, cause a denial of service (reboot) via a request to scripts/commands/reboot, or cause a denial of service (shutdown) via a request to scripts/commands/shutdown.	2014-05-17	8.5	CVE-2014-2084
x2go -- x2go_server	x2gocleansessions in X2Go Server before 4.0.0.8 and 4.0.1.x before 4.0.1.10 allows remote authenticated users to gain privileges via unspecified vectors, possibly related to backticks.	2014-05-20	9.0	CVE-2013-7383
yokogawa -- b/m9000_vp_software	Stack-based buffer overflow in BKESimmgr.exe in the Expanded Test Functions package in Yokogawa CENTUM CS 1000, CENTUM CS 3000 Entry Class R3.09.50 and earlier, CENTUM VP R5.03.00 and earlier, CENTUM VP Entry Class R5.03.00 and earlier, Exaopc R3.71.02 and earlier, B/M9000CS R5.05.01 and earlier, and B/M9000 VP R7.03.01 and earlier allows remote attackers to execute arbitrary code via a crafted packet.	2014-05-16	8.3	CVE-2014-0782

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1323
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1324
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1326
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1327
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1329
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1330

apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1331
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1333
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1334
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1335
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1336
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1337
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute	2014-05-22	6.8	CVE-2014-1338

	arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.			
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1339
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1341
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1342
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1343
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2014-05-21-1.	2014-05-22	6.8	CVE-2014-1344
apple -- safari	WebKit, as used in Apple Safari before 6.1.4 and 7.x before 7.0.4, does not properly interpret Unicode encoding, which allows remote attackers to spoof a postMessage origin, and bypass intended	2014-05-22	5.0	CVE-2014-1346

	restrictions on sending a message to a connected frame or window, via crafted characters in a URL.			
apple -- itunes	Apple iTunes before 11.2.1 on OS X sets world-writable permissions for /Users and /Users/Shared during reboots, which allows local users to modify files, and consequently obtain access to arbitrary user accounts, via standard filesystem operations.	2014-05-18	4.4	CVE-2014-1347
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) blog, (2) bloggeruser, or (3) bloggerpasswd parameter to private/manage/.	2014-05-21	4.3	CVE-2014-3807
barracudadrive -- barracudadrive	Multiple cross-site scripting (XSS) vulnerabilities in BarracudaDrive before 6.7.2 allow remote attackers to inject arbitrary web script or HTML via the (1) role parameter to roles.lsp, (2) name parameter to user.lsp, (3) path parameter to wizard/setuser.lsp, (4) host parameter to tunnelconstr.lsp, or (5) newpath parameter to wfsconstr.lsp in rtl/protected/admin/.	2014-05-21	4.3	CVE-2014-3808
beetel -- 450tc2_router	Cross-site request forgery (CSRF) vulnerability in Beetel 450TC2 Router with firmware TX6-0Q-005_retail allows remote attackers to hijack the authentication of administrators for requests that change the administrator password via the uiViewTools_Password and uiViewTools_PasswordConfirm parameters to Forms/tools_admin_1.	2014-05-20	6.8	CVE-2014-3792
bizagi -- business_process_ management_suite	Cross-site scripting (XSS) vulnerability in Login.aspx in Bizagi BPM Suite before 10.3 allows remote attackers to inject arbitrary web script or HTML via the txtUsername parameter.	2014-05-22	4.3	CVE-2014-2947
bizagi -- business_process_ management_suite	SQL injection vulnerability in workflowenginesoa.asmx in Bizagi BPM Suite through 10.4 allows remote authenticated users to execute arbitrary SQL commands via a crafted SOAP request.	2014-05-22	6.5	CVE-2014-2948
cisco -- nx-os	Directory traversal vulnerability in the command-	2014-05-20	4.6	CVE-2013-6975

	line interface in Cisco NX-OS 6.2(2a) and earlier allows local users to read arbitrary files via unspecified input, aka Bug ID CSCul05217.			
cisco -- unified_web_and_e-mail_interaction_manager	Cross-site scripting (XSS) vulnerability in Cisco Unified Web and E-mail Interaction Manager 9.0(2) allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka Bug ID CSCuj43033.	2014-05-20	4.3	CVE-2014-2192
cisco -- unified_web_and_e-mail_interaction_manager	Cisco Unified Web and E-Mail Interaction Manager places session identifiers in GET requests, which allows remote attackers to inject conversation text by obtaining a valid identifier, aka Bug ID CSCuj43084.	2014-05-20	4.3	CVE-2014-2193
cisco -- unified_web_and_e-mail_interaction_manager	system/egain/chat/entrypoint in Cisco Unified Web and E-mail Interaction Manager 9.0(2) allows remote attackers to have an unspecified impact by injecting a spoofed XML external entity.	2014-05-20	6.8	CVE-2014-2194
cisco -- content_security_management_appliance	Cisco AsyncOS on Email Security Appliance (ESA) and Content Security Management Appliance (SMA) devices, when Active Directory is enabled, does not properly handle group names, which allows remote attackers to gain role privileges by leveraging group-name similarity, aka Bug ID CSCum86085.	2014-05-20	4.3	CVE-2014-2195
cisco -- webex_business_suite	meetinginfo.do in Cisco WebEx Event Center, WebEx Meeting Center, WebEx Sales Center, WebEx Training Center, WebEx Meetings Server 1.5(.1.131) and earlier, and WebEx Business Suite (WBS) 27 before 27.32.31.16, 28 before 28.12.13.18, and 29 before 29.5.1.12 allows remote attackers to obtain sensitive meeting information by leveraging knowledge of a meeting identifier, aka Bug IDs CSCuo68624 and CSCue46738.	2014-05-20	5.0	CVE-2014-2199
cisco -- adaptive_security_appliance_software	Cisco Adaptive Security Appliance (ASA) Software 9.1(.5) and earlier allows remote authenticated users to cause a denial of service (device reload) via crafted attributes in a RADIUS packet, aka Bug ID	2014-05-20	6.3	CVE-2014-3264

	CSCun69561.			
cisco -- security_manager	Cross-site scripting (XSS) vulnerability in the Auto Update Server (AUS) web framework in Cisco Security Manager 4.2 and earlier allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka Bug ID CSCuo06900.	2014-05-20	4.3	CVE-2014-3265
cisco -- unified_border_element	Cisco IOS 15.2(4)M4 on Cisco Unified Border Element (CUBE) devices allows remote attackers to cause a denial of service (input-queue consumption and traffic-processing outage) via crafted RTCP packets, aka Bug ID CSCuj72215.	2014-05-20	5.0	CVE-2014-3268
cisco -- ios_xe	The SNMP module in Cisco IOS XE 3.5E allows remote authenticated users to cause a denial of service (device reload) by polling frequently, aka Bug ID CSCug65204.	2014-05-20	6.8	CVE-2014-3269
cisco -- ios_xr	The DHCPv6 implementation in Cisco IOS XR allows remote attackers to cause a denial of service (process hang) via a malformed packet, aka Bug ID CSCul80924.	2014-05-20	5.0	CVE-2014-3270
cisco -- ios_xr	The DHCPv6 implementation in Cisco IOS XR allows remote attackers to cause a denial of service (device crash) via a malformed packet, aka Bug IDs CSCum85558, CSCum20949, CSCul61849, and CSCul71149.	2014-05-20	5.0	CVE-2014-3271
cisco -- ios	The LLDP implementation in Cisco IOS allows remote attackers to cause a denial of service (device reload) via a malformed packet, aka Bug ID CSCum96282.	2014-05-20	6.1	CVE-2014-3273
dotclear -- dotclear	SQL injection vulnerability in admin/categories.php in Dotclear before 2.6.3 allows remote authenticated users with the manage categories permission to execute arbitrary SQL commands via the categories_order parameter.	2014-05-22	6.5	CVE-2014-3783
emerson -- deltav	Emerson DeltaV 10.3.1, 11.3, 11.3.1, and 12.3 allows local users to modify or read configuration files by leveraging engineering-level privileges.	2014-05-22	4.6	CVE-2014-2349
flag_module_projec	Eval injection vulnerability in the	2014-05-17	6.5	CVE-2014-3453

t -- flag	flag_import_form_validate function in includes/flag.export.inc in the Flag module 7.x-3.0, 7.x-3.5, and earlier for Drupal allows remote authenticated administrators to execute arbitrary PHP code via the "Flag import code" text area to admin/structure/flags/import. NOTE: this issue could also be exploited by other attackers if the administrator ignores a security warning on the permissions assignment page.			
flying_cart -- flying_cart	Cross-site scripting (XSS) vulnerability in Flying Cart allows remote attackers to inject arbitrary web script or HTML via the p parameter to index.php.	2014-05-22	4.3	CVE-2014-3846
gitlab -- gitlab	The Grit gem for Ruby, as used in GitLab 5.2 before 5.4.1 and 6.x before 6.2.3, allows remote authenticated users to execute arbitrary commands, as demonstrated by the search box for the GitLab code search feature.	2014-05-17	6.5	CVE-2013-4489
google -- chrome	The InMemoryUrlProtocol::Read function in media/filters/in_memory_url_protocol.cc in Google Chrome before 35.0.1916.114 relies on an insufficiently large integer data type, which allows remote attackers to cause a denial of service (out-of-bounds read) via vectors that trigger use of a large buffer.	2014-05-21	5.0	CVE-2014-1746
google -- chrome	Cross-site scripting (XSS) vulnerability in the DocumentLoader::maybeCreateArchive function in core/loader/DocumentLoader.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to inject arbitrary web script or HTML via crafted MHTML content, aka "Universal XSS (UXSS)."	2014-05-21	4.3	CVE-2014-1747
google -- chrome	The ScrollView::paint function in platform/scroll/ScrollView.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to spoof the UI by extending scrollbar painting into the parent frame.	2014-05-21	5.0	CVE-2014-1748
google -- chrome	The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote	2014-05-21	4.3	CVE-2014-3803

	attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -x-webkit-speech attribute.			
hp -- icewall_mcrp	Unspecified vulnerability in HP IceWall SSO 10.0 Dfw and IceWall MCRP 2.1 and 3.0 allows remote attackers to cause a denial of service via unknown vectors.	2014-05-22	5.0	CVE-2014-2604
ibm -- websphere_portal	IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0 through 7.0.0.2 CF28, and 8.0 before 8.0.0.1 CF12 allows remote attackers to cause a denial of service (resource consumption and daemon crash) via a crafted web request.	2014-05-22	5.0	CVE-2014-0949
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in FilterForm.jsp in IBM WebSphere Portal 7.0 before 7.0.0.2 CF28 and 8.0 before 8.0.0.1 CF12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-22	4.3	CVE-2014-0951
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in boot_config.jsp in IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF28, 7.0 through 7.0.0.2 CF28, and 8.0 before 8.0.0.1 CF12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-22	4.3	CVE-2014-0952
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in IBM WebSphere Portal 8.0 before 8.0.0.1 CF12, when Social Rendering in Connections integration is enabled, allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	2014-05-22	4.3	CVE-2014-0955
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in googlemap.jsp in IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0 through 7.0.0.2 CF28, and 8.0 before 8.0.0.1 CF12 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-22	4.3	CVE-2014-0956
ibm -- websphere_portal	Open redirect vulnerability in IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0 through 7.0.0.2 CF28, and 8.0	2014-05-22	4.3	CVE-2014-0958

	before 8.0.0.1 CF12 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.			
ibm -- websphere_portal	IBM WebSphere Portal 6.1.0 through 6.1.0.6 CF27, 6.1.5 through 6.1.5.3 CF27, 7.0 through 7.0.0.2 CF28, and 8.0 before 8.0.0.1 CF12 allows remote authenticated users to cause a denial of service (infinite loop) via a login redirect.	2014-05-22	4.0	CVE-2014-0959
imember360 -- imember360	Multiple cross-site scripting (XSS) vulnerabilities in the iMember360 plugin 3.8.012 through 3.9.001 for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) decrypt or (2) encrypt parameter.	2014-05-22	4.3	CVE-2014-3842
intel -- ideo_video	ir41_32.ax 4.51.16.3 for Intel Ideo Video 4.5 allows remote attackers to cause a denial of service (crash) via a crafted .avi file.	2014-05-19	4.3	CVE-2014-3735
k-litecodec -- k-lite_codec	Filters\LAV\avfilter-lav-4.dll in K-lite Codec 10.4.5 and earlier allows remote attackers to cause a denial of service (crash) via a crafted .jpg file.	2014-05-16	4.3	CVE-2014-3452
livezilla -- livezilla	LiveZilla before 5.1.2.1 includes the operator password in plaintext in Javascript code that is generated by lz/mobile/chat.php, which might allow remote attackers to obtain sensitive information and gain privileges by accessing the loginName and loginPassword variables using an independent cross-site scripting (XSS) attack.	2014-05-19	4.3	CVE-2013-7033
livezilla -- livezilla	LiveZilla 5.1.2.1 and earlier includes the MD5 hash of the operator password in plaintext in Javascript code that is generated by lz/mobile/chat.php, which allows remote attackers to obtain sensitive information and gain privileges by accessing the loginName and loginPassword variables using an independent cross-site scripting (XSS) attack. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-7033.	2014-05-19	6.8	CVE-2013-7385
mahara -- mahara	Mahara before 1.5.12, 1.6.x before 1.6.7, and 1.7.x before 1.7.3 does not properly restrict access to artefacts, which allows remote authenticated users	2014-05-19	4.0	CVE-2013-4429

	to read arbitrary artefacts via the (1) artefact id in an upload action when creating a journal or (2) instconf_artefactid_selected[ID] parameter in an upload action when editing a block.			
mahara -- mahara	Cross-site scripting (XSS) vulnerability in Mahara before 1.5.12, 1.6.x before 1.6.7, and 1.7.x before 1.7.3 allows remote attackers to inject arbitrary web script or HTML via the Host header to lib/web.php.	2014-05-19	4.3	CVE-2013-4430
mahara -- mahara	Mahara before 1.5.12, 1.6.x before 1.6.7, and 1.7.x before 1.7.3 does not properly prevent access to blocks, which allows remote authenticated users to modify arbitrary blocks via the bock id in an edit request.	2014-05-19	5.5	CVE-2013-4431
mahara -- mahara	Mahara before 1.5.13, 1.6.x before 1.6.8, and 1.7.x before 1.7.4 does not properly restrict access to folders, which allows remote authenticated users to read arbitrary folders (1) by leveraging an active folder tab loaded before permissions were removed or (2) via the folder parameter to artefact/file/groupfiles.php.	2014-05-19	4.0	CVE-2013-4432
mail_on_update_project -- mail_on_update	Cross-site request forgery (CSRF) vulnerability in the Mail On Update plugin before 5.2.0 for WordPress allows remote attackers to hijack the authentication of administrators for requests that change the "List of alternative recipients" via the mailonupdate_mailto parameter in the mail-on-update page to wp-admin/options-general.php. NOTE: a third party claims that 5.2.1 and 5.2.2 are also vulnerable, but the issue might require a separate CVE identifier since this might reflect an incomplete fix.	2014-05-22	6.8	CVE-2013-2107
microsoft -- debug_interface_access_software_development_kit	msdia.dll in Microsoft Debug Interface Access (DIA) SDK, as distributed in Microsoft Visual Studio before 2013, does not properly validate an unspecified variable before use in calculating a dynamic-call address, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDB file.	2014-05-20	6.8	CVE-2014-3802

netiq -- sentinel	Directory traversal vulnerability in the DumpToFile method in the NQMcsVarSet ActiveX control in Agent Manager in NetIQ Sentinel allows remote attackers to create arbitrary files, and consequently execute arbitrary code, via a crafted pathname.	2014-05-20	6.8	CVE-2014-3460
opentext -- exceed_ondemand	OpenText Exceed OnDemand (EoD) 8 uses weak encryption for passwords, which makes it easier for (1) remote attackers to discover credentials by sniffing the network or (2) local users to discover credentials by reading a .eod8 file.	2014-05-19	5.0	CVE-2013-6805
opentext -- exceed_ondemand	OpenText Exceed OnDemand (EoD) 8 allows man-in-the-middle attackers to disable bidirectional authentication and obtain sensitive information via a crafted string in a response, which triggers a downgrade to simple authentication that sends credentials in plaintext.	2014-05-19	6.8	CVE-2013-6806
opentext -- exceed_ondemand	The client in OpenText Exceed OnDemand (EoD) 8 supports anonymous ciphers by default, which allows man-in-the-middle attackers to bypass server certificate validation, redirect a connection, and obtain sensitive information via crafted responses.	2014-05-19	6.8	CVE-2013-6807
opentext -- exceed_ondemand	OpenText Exceed OnDemand (EoD) 8 transmits the session ID in cleartext, which allows remote attackers to perform session fixation attacks by sniffing the network.	2014-05-19	6.4	CVE-2013-6994
pocoo -- jinja2	FileSystemBytecodeCache in Jinja2 2.7.2 does not properly create temporary directories, which allows local users to gain privileges by pre-creating a temporary directory with a user's uid. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-1402.	2014-05-19	4.4	CVE-2014-0012
pocoo -- jinja2	The default configuration for bccache.FileSystemBytecodeCache in Jinja2 before 2.7.2 does not properly create temporary files, which allows local users to gain privileges via a crafted .cache file with a name starting with __jinja2_ in /tmp.	2014-05-19	4.4	CVE-2014-1402

python -- python	Python 2.7 before 3.4 only uses the last eight bits of the prefix to randomize hash values, which causes it to compute hash values without restricting the ability to trigger hash collisions predictably and makes it easier for context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1150.	2014-05-19	4.3	CVE-2013-7040
quick_tabs_module_project -- quicktabs	The Quick Tabs module 6.x-2.x before 6.x-2.2, 6.x-3.x before 6.x-3.2, and 7.x-3.x before 7.x-3.6 for Drupal does not properly check block permissions, which allows remote attackers to obtain sensitive information by reading a Quick Tab.	2014-05-19	5.0	CVE-2013-4406
sap -- netweaver	SAP NetWeaver 7.20 and earlier allows remote attackers to read arbitrary SAP Central User Administration (SAP CUA) tables via unspecified vectors.	2014-05-19	5.0	CVE-2014-3787
seopanel -- seo_panel	Multiple cross-site scripting (XSS) vulnerabilities in Seo Panel before 3.5.0 allow remote attackers to inject arbitrary web script or HTML via the (1) capcheck parameter to directories.php or (2) keyword parameter to proxy.php.	2014-05-20	4.3	CVE-2014-1855
spumko_project -- hapi_server_framework	The hapi server framework 2.0.x and 2.1.x before 2.2.0 for Node.js allows remote attackers to cause a denial of service (file descriptor consumption and process crash) via unspecified vectors.	2014-05-16	5.0	CVE-2014-3742
tech-banker -- contact_bank	Cross-site scripting (XSS) vulnerability in the Contact Bank plugin before 2.0.20 for WordPress allows remote attackers to inject arbitrary web script or HTML via the Label field, related to form layout configuration. NOTE: some of these details are obtained from third party information.	2014-05-22	4.3	CVE-2014-3841
tinymce -- color_picker	The TinyMCE Color Picker plugin before 1.2 for WordPress does not properly check permissions, which allows remote attackers to modify plugin settings via unspecified vectors. NOTE: some of these details are obtained from third party	2014-05-22	5.0	CVE-2014-3844

	information.			
tinymce -- color_picker	Cross-site request forgery (CSRF) vulnerability in the TinyMCE Color Picker plugin before 1.2 for WordPress allows remote attackers to hijack the authentication of unspecified users for requests that change plugin settings via unknown vectors. NOTE: some of these details are obtained from third party information.	2014-05-22	6.8	CVE-2014-3845
typo3 -- typo3	The Backend History Module in TYPO3 4.5.x before 4.5.21, 4.6.x before 4.6.14, and 4.7.x before 4.7.6 does not properly restrict access, which allows remote authenticated editors to read the history of arbitrary records via a crafted URL.	2014-05-20	4.0	CVE-2012-6146
typo3 -- typo3	The (1) file upload component and (2) File Abstraction Layer (FAL) in TYPO3 6.0.x before 6.0.8 and 6.1.x before 6.1.3 does not properly check file extensions, which allows remote authenticated editors to execute arbitrary PHP code by uploading a .php file.	2014-05-20	6.5	CVE-2013-4250
typo3 -- typo3	The File Abstraction Layer (FAL) in TYPO3 6.0.x before 6.0.9 and 6.1.x before 6.1.4 does not properly check permissions, which allows remote authenticated users to create or read arbitrary files via a crafted URL.	2014-05-20	5.5	CVE-2013-4320
typo3 -- typo3	The File Abstraction Layer (FAL) in TYPO3 6.0.x before 6.0.8 and 6.1.x before 6.1.4 allows remote authenticated editors to execute arbitrary PHP code via unspecified characters in the file extension when renaming a file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4250.	2014-05-20	6.5	CVE-2013-4321
unrealircd -- unrealircd	Use-after-free vulnerability in UnrealIRCd 3.2.10 before 3.2.10.2 allows remote attackers to cause a denial of service (crash) via unspecified vectors. NOTE: this identifier was SPLIT per ADT2 due to different vulnerability types. CVE-2013-7384 was assigned for the NULL pointer dereference.	2014-05-19	5.0	CVE-2013-6413
unrealircd -- unrealircd	UnrealIRCd 3.2.10 before 3.2.10.2 allows remote attackers to cause a denial of service (NULL pointer	2014-05-19	5.0	CVE-2013-7384

	dereference and crash) via unspecified vectors, related to SSL. NOTE: this issue was SPLIT from CVE-2013-6413 per ADT2 due to different vulnerability types.			
urbanairship -- python-oauth2	The Server.verify_request function in SimpleGeo python-oauth2 does not check the nonce, which allows remote attackers to perform replay attacks via a signed URL.	2014-05-20	4.3	CVE-2013-4346
urbanairship -- python-oauth2	The (1) make_nonce, (2) generate_nonce, and (3) generate_verifier functions in SimpleGeo python-oauth2 uses weak random numbers to generate nonces, which makes it easier for remote attackers to guess the nonce via a brute force attack.	2014-05-20	5.8	CVE-2013-4347
vicidial -- vicidial	VICIDIAL dialer (aka Asterisk GUI client) 2.8-403a, 2.7, 2.7RC1, and earlier has a hardcoded password of donotedit for the (1) VDAD and (2) VDCL users, which makes it easier for remote attackers to obtain access.	2014-05-17	5.0	CVE-2013-7382
vmturbo -- operations_manager	Directory traversal vulnerability in cgi-bin/help/dolt.cgi in VMTurbo Operations Manager before 4.6 allows remote attackers to read arbitrary files via a .. (dot dot) in the xml_path parameter.	2014-05-21	5.0	CVE-2014-3806
wordpress -- booking_system	SQL injection vulnerability in dopbs-backend-forms.php in the Booking System (Booking Calendar) plugin before 1.3 for WordPress allows remote authenticated users to execute arbitrary SQL commands via the booking_form_id parameter to wp-admin/admin-ajax.php.	2014-05-22	6.5	CVE-2014-3210
zemanta -- search_everything	Cross-site request forgery (CSRF) vulnerability in the Search Everything plugin before 8.1.1 for WordPress allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.	2014-05-22	6.8	CVE-2014-3843
zenoss -- zenoss	Cross-site scripting (XSS) vulnerability in Zenoss 4.2.5 allows remote attackers to inject arbitrary web script or HTML via the title of a device.	2014-05-20	4.3	CVE-2014-3738
zenoss -- zenoss	Open redirect vulnerability in zport/acl_users/cookieAuthHelper/login_form in	2014-05-20	5.8	CVE-2014-3739

	Zenoss 4.2.5 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the came_from parameter.			

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
florian_weber -- spaces	The Spaces OG submodule in the Spaces module 6.x-3.x before 6.x-3.7 for Drupal does not properly delete organic group group spaces content when using the option to move to a new group, which causes the content to be "orphaned" and allows remote authenticated users with the "access content" permission to obtain sensitive information via vectors involving a rebuild access for the site or content.	2014-05-17	2.1	CVE-2013-4498
gdm-guest-session_project -- gdm-guest-session	gdm/guest-session-cleanup.sh in gdm-guest-session 0.24 and earlier, as used in Ubuntu Linux 10.04 LTS, 10.10, and 11.04, allows local users to delete arbitrary files via a space in the name of a file in /tmp. NOTE: this identifier was SPLIT from CVE-2012-0943 per ADT1/ADT2 due to different codebases and affected versions. CVE-2012-0943 is used for the guest-account issue.	2014-05-22	2.1	CVE-2012-6648
gnome -- gnome-terminal	The "insert-blank-characters" capability in caps.c in gnome-terminal (vte) before 0.28.1 allows remote authenticated users to cause a denial of service (CPU and memory consumption and crash) via a crafted file, as demonstrated by a file containing the string,	2014-05-21	3.5	CVE-2011-2198

	"\033[10000000000000000@".			
leon_weber -- pyxtrlock	pyxtrlock before 0.1 uses an incorrect variable name, which allows physically proximate attackers to bypass the lock screen via multiple failed authentication attempts, which trigger a crash.	2014-05-19	3.6	CVE-2013-4426
leon_weber -- pyxtrlock	pyxtrlock before 0.2 does not properly check the return values of the (1) xcb_grab_pointer and (2) xcb_grab_keyboard XCB library functions, which allows physically proximate attackers to gain access to the keyboard or mouse without unlocking the screen via unspecified vectors.	2014-05-19	2.1	CVE-2013-4427
mediafront -- mediafront	Cross-site scripting (XSS) vulnerability in the MediaFront module 6.x-1.x before 6.x-1.6, 7.x-1.x before 7.x-1.6, and 7.x-2.x before 7.x-2.1 for Drupal allows remote authenticated users with the "administer mediafront" permission to inject arbitrary web script or HTML via the preset settings.	2014-05-20	2.1	CVE-2013-4380
robert_ancell -- lightdm	debian/guest-account in Light Display Manager (lightdm) 1.0.x before 1.0.6 and 1.1.x before 1.1.7, as used in Ubuntu Linux 11.10, allows local users to delete arbitrary files via a space in the name of a file in /tmp. NOTE: this identifier was SPLIT per ADT1/ADT2 due to different codebases and affected versions. CVE-2012-6648 has been assigned for the gdm-guest-session issue.	2014-05-22	2.1	CVE-2012-0943
xen -- xen	The ARM image loading functionality in Xen 4.4.x does not properly validate kernel length, which allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit ARM guest kernel in an image, which triggers a buffer overflow.	2014-05-19	3.3	CVE-2014-3714
xen -- xen	Buffer overflow in Xen 4.4.x allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit guest kernel, related to searching for an appended DTB.	2014-05-19	3.3	CVE-2014-3715
xen -- xen	Xen 4.4.x does not properly check alignment, which allows local users to cause a denial of service (crash) via an unspecified field in a DTB header in a 32-bit	2014-05-19	1.9	CVE-2014-3716

	guest kernel.			
xen -- xen	Xen 4.4.x does not properly validate the load address for 64-bit ARM guest kernels, which allows local users to read system memory or cause a denial of service (crash) via a crafted kernel, which triggers a buffer overflow.	2014-05-19	3.3	CVE-2014-3717
florian_weber -- spaces	The Spaces OG submodule in the Spaces module 6.x-3.x before 6.x-3.7 for Drupal does not properly delete organic group group spaces content when using the option to move to a new group, which causes the content to be "orphaned" and allows remote authenticated users with the "access content" permission to obtain sensitive information via vectors involving a rebuild access for the site or content.	2014-05-17	2.1	CVE-2013-4498
gdm-guest-session_project -- gdm-guest-session	gdm/guest-session-cleanup.sh in gdm-guest-session 0.24 and earlier, as used in Ubuntu Linux 10.04 LTS, 10.10, and 11.04, allows local users to delete arbitrary files via a space in the name of a file in /tmp. NOTE: this identifier was SPLIT from CVE-2012-0943 per ADT1/ADT2 due to different codebases and affected versions. CVE-2012-0943 is used for the guest-account issue.	2014-05-22	2.1	CVE-2012-6648
gnome -- gnome-terminal	The "insert-blank-characters" capability in caps.c in gnome-terminal (vte) before 0.28.1 allows remote authenticated users to cause a denial of service (CPU and memory consumption and crash) via a crafted file, as demonstrated by a file containing the string, "\033[10000000000000000@".	2014-05-21	3.5	CVE-2011-2198
leon_weber -- pyxtrlock	pyxtrlock before 0.1 uses an incorrect variable name, which allows physically proximate attackers to bypass the lock screen via multiple failed authentication attempts, which trigger a crash.	2014-05-19	3.6	CVE-2013-4426
leon_weber -- pyxtrlock	pyxtrlock before 0.2 does not properly check the return values of the (1) xcb_grab_pointer and (2) xcb_grab_keyboard XCB library functions, which allows physically proximate attackers to gain access to the keyboard or mouse without unlocking the	2014-05-19	2.1	CVE-2013-4427

	screen via unspecified vectors.			
mediafront -- mediafront	Cross-site scripting (XSS) vulnerability in the MediaFront module 6.x-1.x before 6.x-1.6, 7.x-1.x before 7.x-1.6, and 7.x-2.x before 7.x-2.1 for Drupal allows remote authenticated users with the "administer mediafront" permission to inject arbitrary web script or HTML via the preset settings.	2014-05-20	2.1	CVE-2013-4380
robert_ancell -- lightdm	debian/guest-account in Light Display Manager (lightdm) 1.0.x before 1.0.6 and 1.1.x before 1.1.7, as used in Ubuntu Linux 11.10, allows local users to delete arbitrary files via a space in the name of a file in /tmp. NOTE: this identifier was SPLIT per ADT1/ADT2 due to different codebases and affected versions. CVE-2012-6648 has been assigned for the gdm-guest-session issue.	2014-05-22	2.1	CVE-2012-0943
xen -- xen	The ARM image loading functionality in Xen 4.4.x does not properly validate kernel length, which allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit ARM guest kernel in an image, which triggers a buffer overflow.	2014-05-19	3.3	CVE-2014-3714
xen -- xen	Buffer overflow in Xen 4.4.x allows local users to read system memory or cause a denial of service (crash) via a crafted 32-bit guest kernel, related to searching for an appended DTB.	2014-05-19	3.3	CVE-2014-3715
xen -- xen	Xen 4.4.x does not properly check alignment, which allows local users to cause a denial of service (crash) via an unspecified field in a DTB header in a 32-bit guest kernel.	2014-05-19	1.9	CVE-2014-3716
xen -- xen	Xen 4.4.x does not properly validate the load address for 64-bit ARM guest kernels, which allows local users to read system memory or cause a denial of service (crash) via a crafted kernel, which triggers a buffer overflow.	2014-05-19	3.3	CVE-2014-3717

- 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