UgCERT Computer Emergency Response Team

UGANDA COMMUNICATIONS COMMISSION

Vulnerability Summary for the Week of June 2, 2014

Please Note:

- The vulnerabilities are categorized 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
ajaydsouza -- contextual_related_posts	SQL injection vulnerability in the Contextual Related Posts plugin before 1.8.10.2 for WordPress allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2014-06-02	7.5	CVE-2014-3937
aten -- cn8000	The ATEN CN8000 remote-access unit with firmware 1.6.154 and earlier allows remote attackers to cause a denial of service via unspecified vectors.	2014-06-05	7.8	CVE-2014-1997
bitrix -- bitrix_e-store_module	The Bitrix e-Store module before 14.0.1 for Bitrix Site Manager uses sequential values for the BITRIX_SM_SALE_UID cookie, which makes it easier for remote attackers to guess the cookie value and bypass authentication via a brute force attack.	2014-05-30	7.5	CVE-2013-6788
citrix -- vdi-in-a-box	Unspecified vulnerability in Citrix VDI-In-A-Box 5.3.x before 5.3.8 and 5.4.x before 5.4.4 allows remote attackers to bypass authentication via unspecified vectors, related to a Java servlet.	2014-05-30	7.5	CVE-2014-3780
copadata --	COPA-DATA zenon DNP3 NG driver (DNP3	2014-06-05	7.1	CVE-2014-2345

zenon_dnp3_ng_driver	master) 7.10 and 7.11 through 7.11 SP0 build 10238 and zenon DNP3 Process Gateway (DNP3 outstation) 7.11 SP0 build 10238 and earlier allow remote attackers to cause a denial of service (infinite loop and process crash) by sending a crafted DNP3 packet over TCP.			
corel -- paintshop_pro_x5	Untrusted search path vulnerability in Corel PaintShop Pro X5 and X6 16.0.0.113, 15.2.0.2, and earlier allows local users to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse dwmapi.dll that is located in the same folder as a .jpg file.	2014-06-05	9.3	CVE-2013-0733
cososys -- endpoint_protector	SQL injection vulnerability in the device registration component in wsf/webservice.php in CoSoSys Endpoint Protector 4 4.3.0.4 and 4.4.0.2 allows remote attackers to execute arbitrary SQL commands via unspecified parameters.	2014-06-02	7.5	CVE-2014-3932
d-link -- dir-505l_shareport_mobile_companion	Stack-based buffer overflow in the do_hnap function in www/my_cgi.cgi in D-Link DSP-W215 (Rev. A1) with firmware 1.01b06 and earlier, DIR-505 with firmware before 1.08b10, and DIR-505L with firmware 1.01 and earlier allows remote attackers to execute arbitrary code via a long Content-Length header in a GetDeviceSettings action in an HNAP request.	2014-06-02	10.0	CVE-2014-3936
dell -- powervault_ml6000	logViewer.htm on the Dell ML6000 tape backup system with firmware before i8.2.0.2 (641G.GS103) and the Quantum Scalar i500 tape backup system with firmware before i8.2.2.1 (646G.GS002) allows remote attackers to execute arbitrary commands via shell metacharacters in a pathname parameter.	2014-06-02	9.0	CVE-2014-2959
dleviet -- datalife_engine	DataLife Engine (DLE) 9.7 allows remote attackers to execute arbitrary PHP code via the catlist[] parameter to engine/preview.php, which is used in a preg_replace function call with an e modifier.	2014-06-02	7.5	CVE-2013-1412

emc -- documentum_digital_asset_manager	The thumbnail proxy server in EMC Documentum Digital Asset Manager (DAM) 6.5 SP3, 6.5 SP4, 6.5 SP5, and 6.5 SP6 before P13 allows remote attackers to conduct Documentum Query Language (DQL) injection attacks and bypass intended restrictions on querying objects via a crafted parameter in a query string.	2014-06-05	7.5	CVE-2014-2503
ericom -- accessnow_server	Stack-based buffer overflow in AccessServer32.exe in Ericom AccessNow Server allows remote attackers to execute arbitrary code via a request for a non-existent file.	2014-06-04	10.0	CVE-2014-3913
frontaccounting -- frontaccounting	Multiple SQL injection vulnerabilities in FrontAccounting (FA) before 2.3.21 allow remote attackers to execute arbitrary SQL commands via unspecified vectors.	2014-06-05	7.5	CVE-2014-3973
fruux -- sabredav	SabreDAV before 1.7.11, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2014-06-04	7.5	CVE-2014-2055
getid3 -- getid3	getID3() before 1.9.8, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2014-06-04	7.5	CVE-2014-2053
ibm -- db2	Multiple untrusted search path vulnerabilities in unspecified (1) setuid and (2) setgid programs in IBM DB2 9.5, 9.7 before FP9a, 9.8, 10.1 before FP3a, and 10.5 before FP3a on Linux and UNIX allow local users to gain root privileges via a Trojan horse library.	2014-05-30	7.2	CVE-2014-0907
ingy -- spoon	Spoon::Cookie in the Spoon module 0.24 for Perl does not properly use the Storable::thaw function, which allows remote attackers to execute arbitrary code via a crafted request, which is not properly handled when it is deserialized.	2014-06-04	7.5	CVE-2012-6143

jochen_wiedmann -- html::ep	Session::Cookie in the HTML::EP module 0.2011 for Perl does not properly use the Storable::thaw function, which allows remote attackers to execute arbitrary code via a crafted request, which is not properly handled when it is deserialized.	2014-06-04	7.5	CVE-2012-6142
openstack -- neutron	The default configuration in the Red Hat openstack-neutron package before 2013.2.3-7 does not properly set a configuration file for rootwrap, which allows remote attackers to gain privileges via a crafted configuration file.	2014-06-02	7.6	CVE-2013-6433
owncloud -- owncloud	ownCloud Server before 5.0.15 and 6.0.x before 6.0.2 allows remote attackers to conduct an LDAP injection attack via unspecified vectors, as demonstrated using a "login query."	2014-06-05	7.5	CVE-2014-2051
owncloud -- owncloud	PHPExcel before 1.8.0, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, does not disable external entity loading in libxml, which allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2014-06-04	7.5	CVE-2014-2054
owncloud -- owncloud	PHPDocX, as used in ownCloud Server before 5.0.15 and 6.0.x before 6.0.2, allows remote attackers to read arbitrary files, cause a denial of service, or possibly have other impact via an XML External Entity (XXE) attack.	2014-06-04	7.5	CVE-2014-2056
owncloud -- owncloud	ownCloud Server before 6.0.3 does not properly check permissions, which allows remote authenticated users to (1) access the contacts of other users via the address book or (2) rename files via unspecified vectors.	2014-06-04	7.5	CVE-2014-3834
phpnuke -- php-nuke	SQL injection vulnerability in the Submit_News module for PHP-Nuke 8.3 allows remote attackers to execute arbitrary SQL commands via the topics[] parameter to modules.php.	2014-06-02	7.5	CVE-2014-3934
radiothermostat -- ct50	Radio Thermostat CT80 And CT50 with firmware 1.4.64 and earlier does not restrict access to the	2014-06-05	8.3	CVE-2013-4860

	API, which allows remote attackers to change the operation mode, wifi connection settings, temperature thresholds, and other settings via unspecified vectors.			
rom_walton -- boinc	Stack-based buffer overflow in BOINC 6.10.58 and 6.12.34 allows remote attackers to have unspecified impact via multiple file_signature elements.	2014-06-02	9.3	CVE-2013-2019
rom_walton -- boinc	Multiple stack-based buffer overflows in the XML parser in BOINC 7.x allow attackers to have unspecified impact via a crafted XML file, related to the scheduler.	2014-06-02	9.3	CVE-2013-2298
samsung -- ipolis_device_manager	Stack-based buffer overflow in the FindConfigChildeKeyList method in the XNSSDKDEVICE.XnsSdkDeviceCtrlForIpInstaller.1 ActiveX control in Samsung iPOLiS Device Manager before 1.8.7 allows remote attackers to execute arbitrary code via a long value.	2014-06-05	9.3	CVE-2014-3912
sensiolabs -- symfony	The Yaml::parse function in Symfony 2.0.x before 2.0.22 remote attackers to execute arbitrary PHP code via a PHP file, a different vulnerability than CVE-2013-1397.	2014-06-02	7.5	CVE-2013-1348
sensiolabs -- symfony	Symfony 2.0.x before 2.0.22, 2.1.x before 2.1.7, and 2.2.x remote attackers to execute arbitrary PHP code via a serialized PHP object to the (1) Yaml::parse or (2) Yaml\Parser::parse function, a different vulnerability than CVE-2013-1348.	2014-06-02	7.5	CVE-2013-1397
stephen_adkins -- app::context	The App::Context module 0.01 through 0.968 for Perl does not properly use the Storable::thaw function, which allows remote attackers to execute arbitrary code via a crafted request to (1) App::Session::Cookie or (2) App::Session::HTMLHidden, which is not properly handled when it is deserialized.	2014-06-04	7.5	CVE-2012-6141
videos_tube_project -- videos_tube	Multiple SQL injection vulnerabilities in Videos Tube 1.0 allow remote attackers to execute arbitrary SQL commands via the url parameter to (1) videocat.php or (2) single.php.	2014-06-04	7.5	CVE-2014-3962

vmware -- vcenter_server_appliance	Ruby vSphere Console (RVC) in VMware vCenter Server Appliance allows remote authenticated users to execute arbitrary commands as root by escaping from a chroot jail.	2014-06-01	9.0	CVE-2014-3790
xen -- xen	Xen 4.4.x, when running on an ARM system, does not properly check write permissions on virtual addresses, which allows local guest administrators to gain privileges via unspecified vectors.	2014-06-05	7.4	CVE-2014-3969
xnau -- participants_database	SQL injection vulnerability in the Export CSV page in the Participants Database plugin before 1.5.4.9 for WordPress allows remote attackers to execute arbitrary SQL commands via the query parameter in an "output CSV" action to pdb-signup/.	2014-06-04	7.5	CVE-2014-3961
xoops -- glossaire_module	SQL injection vulnerability in glossaire-aff.php in the Glossaire module 1.0 for XOOPS allows remote attackers to execute arbitrary SQL commands via the lettre parameter.	2014-06-02	7.5	CVE-2014-3935

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
a10networks -- advanced_core_operating_system	Buffer overflow in A10 Networks Advanced Core Operating System (ACOS) before 2.7.0-p6 and 2.7.1 before 2.7.1-P1_55 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long session id in the URI to sys_reboot.html. NOTE: some of these details are	2014-06-05	5.0	CVE-2014-3976

	obtained from third party information.			
ajaydsouza -- contextual_related_posts	Cross-site request forgery (CSRF) vulnerability in the Contextual Related Posts plugin before 1.8.7 for WordPress allows remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting (XSS) attacks via unspecified vectors.	2014-06-02	6.8	CVE-2013-2710
alex_kellner -- powermail	Cross-site scripting (XSS) vulnerability in the HTML export wizard in the backend module in the powermail extension before 1.6.11 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-04	4.3	CVE-2014-3948
alfresco -- alfresco	Multiple cross-site scripting (XSS) vulnerabilities in Alfresco Enterprise before 4.1.6.13 allow remote attackers to inject arbitrary web script or HTML via (1) an XHTML document, (2) a <% tag, or (3) the taskId parameter to share/page/task-edit.	2014-06-02	4.3	CVE-2014-2939
apache -- tomcat	Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data.	2014-05-31	5.0	CVE-2014-0075
apache -- tomcat	java/org/apache/coyote/ajp/AbstractAjpProcessor.java in Apache Tomcat 8.x before 8.0.4 allows remote attackers to cause a denial of service (thread consumption) by using a "Content-Length: 0" AJP request to trigger a hang in request processing.	2014-05-31	5.0	CVE-2014-0095
apache -- tomcat	java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity	2014-05-31	4.3	CVE-2014-0096

	declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.			
apache -- tomcat	Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.	2014-05-31	4.3	CVE-2014-0099
apache -- tomcat	Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application.	2014-05-31	4.3	CVE-2014-0119
auracms -- auracms	Cross-site scripting (XSS) vulnerability in filemanager.php in AuraCMS 3.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the viewdir parameter.	2014-06-05	4.3	CVE-2014-3974
auracms -- auracms	Absolute path traversal vulnerability in filemanager.php in AuraCMS 3.0 allows remote attackers to list a directory via a full pathname in the viewdir parameter.	2014-06-05	5.0	CVE-2014-3975
bottomline -- transform_foundation_server	Multiple cross-site scripting (XSS) vulnerabilities in the Transform Content Center in Bottomline Technologies Transform Foundation Server before 4.3.1 Patch 8 and 5.x before 5.2 Patch 7 allow remote attackers to inject arbitrary web script or HTML via the (1) pn parameter to index.fsp/document.pdf, (2) db or (3) referer parameter to index.fsp/index.fsp, or (4) PATH_INFO to the default URI.	2014-06-05	4.3	CVE-2014-2577
bufferapp --	Cross-site request forgery (CSRF) vulnerability in he	2014-06-02	6.8	CVE-2013-3258

digg_digg	Digg Digg plugin before 5.3.5 for WordPress allows remote attackers to hijack the authentication of users for requests that modify settings via unspecified vectors.			
cisco -- unified_communications_domain_manager	The web framework in VOSS in Cisco Unified Communications Domain Manager (CDM) 9.0(.1) and earlier does not properly implement access control, which allows remote authenticated users to obtain potentially sensitive user information by visiting an unspecified Administration GUI web page, aka Bug IDs CSCun46045 and CSCun46116.	2014-06-03	4.0	CVE-2014-3280
cogentdatahub -- cogent_datahub	Directory traversal vulnerability in Cogent DataHub before 7.3.5 allows remote attackers to read arbitrary files of unspecified types, or cause a web-server denial of service, via a crafted pathname.	2014-05-30	6.4	CVE-2014-2352
cogentdatahub -- cogent_datahub	Cross-site scripting (XSS) vulnerability in Cogent DataHub before 7.3.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-30	4.3	CVE-2014-2353
cogentdatahub -- cogent_datahub	Cogent DataHub before 7.3.5 does not use a salt during password hashing, which makes it easier for context-dependent attackers to obtain cleartext passwords via a brute-force attack.	2014-05-30	5.0	CVE-2014-2354
copadata -- zenon_dnp3_ng_driver	COPA-DATA zenon DNP3 NG driver (DNP3 master) 7.10 and 7.11 through 7.11 SP0 build 10238 and zenon DNP3 Process Gateway (DNP3 outstation) 7.11 SP0 build 10238 and earlier allow physically proximate attackers to cause a denial of service (infinite loop and process crash) via crafted input over a serial line.	2014-06-05	4.0	CVE-2014-2346
corel -- quattro_pro_x6	The (1) QProGetNotebookWindowHandle and (2) Ordinal132 functions in QPW160.dll in Corel Quattro Pro X6 Standard Edition 16.0.0.388 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted QPW file.	2014-06-05	4.3	CVE-2012-4728
dancer -- dancer	CRLF injection vulnerability in the cookie method (lib/Dancer/Cookie.pm) in Dancer before 1.3114	2014-05-30	5.0	CVE-2012-5572

	allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a cookie name, a different vulnerability than CVE-2012-5526.			
danielkorte -- nodeaccesskeys	The Node Access Keys module 7.x-1.x before 7.x-1.1 for Drupal does not properly check permissions, which allows remote attackers to bypass access restrictions via a node listing.	2014-06-02	5.8	CVE-2013-4596
debian -- dpkg	dpkg 1.15.9, 1.16.x before 1.16.14, and 1.17.x before 1.17.9 expect the patch program to be compliant with a need for the "C-style encoded filenames" feature, but is supported in environments with noncompliant patch programs, which triggers an interaction error that allows remote attackers to conduct directory traversal attacks and modify files outside of the intended directories via a crafted source package. NOTE: this vulnerability exists because of reliance on unrealistic constraints on the behavior of an external program.	2014-05-30	5.0	CVE-2014-3227
debian -- dpkg-dev	Directory traversal vulnerability in dpkg-source in dpkg-dev 1.3.0 allows remote attackers to modify files outside of the intended directories via a crafted source package that lacks a --- header line.	2014-05-30	5.0	CVE-2014-3864
debian -- dpkg-dev	Multiple directory traversal vulnerabilities in dpkg-source in dpkg-dev 1.3.0 allow remote attackers to modify files outside of the intended directories via a source package with a crafted Index: pseudo-header in conjunction with (1) missing --- and +++ header lines or (2) a +++ header line with a blank pathname.	2014-05-30	5.0	CVE-2014-3865
digital_zoom_studio -- video_gallery	Multiple cross-site scripting (XSS) vulnerabilities in the Digital Zoom Studio (DZS) Video Gallery plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the logoLink parameter to (1) preview.swf, (2) preview_skin_rouge.swf, (3) preview_allchars.swf, or (4) preview_skin_overlay.swf in deploy/.	2014-05-30	4.3	CVE-2014-3923
dleviet --	Session fixation vulnerability in DataLife Engine	2014-06-02	6.8	CVE-2013-7387

datalife_engine	(DLE) 9.7 and earlier allows remote attackers to hijack web sessions via the PHPSESSID cookie.			
emc -- rsa_adaptive_authentication_hosted	Cross-site scripting (XSS) vulnerability in rsa_fso.swf in EMC RSA Adaptive Authentication (Hosted) 11.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-04	4.3	CVE-2014-2502
f5 -- big-ip_access_policy_manager	Cross-site scripting (XSS) vulnerability in list.jsp in the Configuration utility in F5 BIG-IP LTM, AFM, Analytics, APM, ASM, GTM, and Link Controller 11.2.1 through 11.5.1, AAM 11.4.0 through 11.5.1 PEM 11.3.0 through 11.5.1, PSM 11.2.1 through 11.4.1, WebAccelerator and WOM 11.2.1 through 11.3.0, and Enterprise Manager 3.0.0 through 3.1.1 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2014-06-03	4.3	CVE-2014-3959
getpixie -- pixie	Multiple cross-site scripting (XSS) vulnerabilities in the contact module (admin/modules/contact.php) in Pixie CMS 1.04 allow remote attackers to inject arbitrary web script or HTML via the (1) uemail or (2) subject parameter in the Contact form to contact/.	2014-06-04	4.3	CVE-2014-3786
gnu -- gnutls	Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.	2014-06-03	6.8	CVE-2014-3466
gnu -- gnutls	Multiple unspecified vulnerabilities in the DER decoder in GNU Libtasn1 before 3.6, as used in GnutTLS, allow remote attackers to cause a denial of service (out-of-bounds read) via a crafted ASN.1 data.	2014-06-05	4.3	CVE-2014-3467
gnu -- gnutls	The asn1_get_bit_der function in GNU Libtasn1 before 3.6 does not properly report an error when a negative bit length is identified, which allows context-dependent attackers to cause out-of-bounds access via crafted ASN.1 data.	2014-06-05	6.8	CVE-2014-3468
gnu -- gnutls	The (1) asn1_read_value_type and (2) asn1_read_value functions in GNU Libtasn1 before	2014-06-05	4.3	CVE-2014-3469

	3.6 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via a NULL value in an ivalue argument.			
huawei -- webui	Cross-site request forgery (CSRF) vulnerability in api/sms/send-sms in the Web UI 11.010.06.01.858 on Huawei E303 modems with software 22.157.18.00.858 allows remote attackers to hijack the authentication of administrators for requests that perform API operations and send SMS messages via a request element in an XML document.	2014-06-02	6.8	CVE-2014-2946
ibm -- db2	The Stored Procedure infrastructure in IBM DB2 9.5, 9.7 before FP9a, 10.1 before FP3a, and 10.5 before FP3a on Windows allows remote authenticated users to gain privileges by leveraging the CONNECT privilege and the CREATE_EXTERNAL_ROUTINE authority.	2014-05-30	6.5	CVE-2013-6744
ibm -- smart_analytics_system_7700	Unspecified vulnerability in IBM Smart Analytics System 7700 before FP 2.1.3.0 and 7710 before FP 2.1.3.0 allows local users to gain privileges via vectors related to events.	2014-06-04	4.6	CVE-2014-0935
ibm -- websphere_service_registry_and_repository	Cross-site scripting (XSS) vulnerability in the Web UI in IBM WebSphere Service Registry and Repository (WSRR) 6.2, 6.3 before 6.3.0.6, 7.0 before 7.0.0.6, 7.5 before 7.5.0.5, and 8.0 before 8.0.0.3 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.	2014-05-30	4.3	CVE-2014-3010
ipswitch -- imail_server	Multiple cross-site scripting (XSS) vulnerabilities in the web client interface in Ipswitch IMail Server 12.3 and 12.4, possibly before 12.4.1.15, allow remote attackers to inject arbitrary web script or HTML via (1) the Name field in an add new contact action in the Contacts section or unspecified vectors in (2) an Add Group task in the Contacts section, (3) an add new event action in the Calendar section, or (4) the Task section.	2014-06-05	4.3	CVE-2014-3878
lucas_clemente_vella -- libpam-pgsql	libpam-pgsql (aka pam_pgsql) 0.7 does not properly handle a NULL value returned by the	2014-06-03	5.0	CVE-2013-0191

	password search query, which allows remote attackers to bypass authentication via a crafted password.			
mediawiki -- mediawiki	Session fixation vulnerability in Special:UserLogin in MediaWiki before 1.18.6, 1.19.x before 1.19.3, and 1.20.x before 1.20.1 allows remote attackers to hijack web sessions via the session_id.	2014-06-02	6.8	CVE-2012-5391
mediawiki -- mediawiki	Session fixation vulnerability in the CentralAuth extension for MediaWiki before 1.18.6, 1.19.x before 1.19.3, and 1.20.x before 1.20.1 allows remote attackers to hijack web sessions via the centralauth_Session cookie.	2014-06-02	6.8	CVE-2012-5395
mediawiki -- mediawiki	maintenance/mwdoc-filter.php in MediaWiki before 1.20.3 allows remote attackers to read arbitrary files via unspecified vectors.	2014-06-02	5.0	CVE-2013-1818
n-i-agroinformatics -- soy_cms	Cross-site scripting (XSS) vulnerability in Nippon Institute of Agroinformatics SOY CMS 1.4.0c and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-05	4.3	CVE-2014-1998
nero -- mediahome	Multiple off-by-one errors in NMMediaServerService.dll in Nero MediaHome 4.5.8.0 and earlier allow remote attackers to cause a denial of service (crash) via a long string in the (1) request line or (2) HTTP Referer header to TCP port 54444, which triggers a heap-based buffer overflow.	2014-05-30	5.0	CVE-2012-5876
nero -- mediahome	Nero MediaHome 4.5.8.0 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an HTTP header without a name.	2014-05-30	5.0	CVE-2012-5877
network-weathermap -- .network_weathermap	Cross-site scripting (XSS) vulnerability in editor.php in Network Weathermap before 0.97b allows remote attackers to inject arbitrary web script or HTML via the map_title parameter.	2014-06-05	4.3	CVE-2013-2618
network-weathermap -- .network_weatherm	Directory traversal vulnerability in editor.php in Network Weathermap 0.97c and earlier allows remote attackers to read arbitrary files via a .. (dot	2014-06-05	5.0	CVE-2013-3739

ap	dot) in the mapname parameter in a show_config action.			
openinfosecfoundation -- suricata	Suricata before 1.4.6 allows remote attackers to cause a denial of service (crash) via a malformed SSL record.	2014-05-30	5.0	CVE-2013-5919
opennms -- opennms	Multiple cross-site scripting (XSS) vulnerabilities in OpenNMS before 1.12.7 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-06-04	4.3	CVE-2014-3960
openssl -- openssl	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	2014-06-05	6.8	CVE-2014-0195
openssl -- openssl	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	2014-06-05	4.3	CVE-2014-0221
openssl -- openssl	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	2014-06-05	6.8	CVE-2014-0224
openssl -- openssl	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering	2014-06-05	4.3	CVE-2014-3470

	a NULL certificate value.			
openstack -- keystone	OpenStack Identity (Keystone) before 2013.1 allows remote attackers to cause a denial of service (memory consumption and crash) via multiple long requests.	2014-06-02	5.0	CVE-2013-2014
owncloud -- owncloud	Multiple cross-site scripting (XSS) vulnerabilities in ownCloud Server before 4.0.8 allow remote attackers to inject arbitrary web script or HTML via the (1) readyCallback parameter to apps/files_odfviewer/src/webodf/webodf/flashput/PUT.swf, the (2) root parameter to apps/gallery/templates/index.php, or a (3) malformed query to lib/db.php.	2014-06-04	4.3	CVE-2012-5056
owncloud -- owncloud	CRLF injection vulnerability in ownCloud Server before 4.0.8 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via the url path parameter.	2014-06-04	4.3	CVE-2012-5057
owncloud -- owncloud	lib/base.php in ownCloud before 4.0.8 does not properly validate the user_id session variable, which allows remote authenticated users to read arbitrary files via vectors related to WebDAV.	2014-06-04	4.0	CVE-2012-5336
owncloud -- owncloud	settings/personal.php in ownCloud 4.5.x before 4.5.6 allows remote authenticated users to execute arbitrary PHP code via crafted mount point settings.	2014-06-04	4.6	CVE-2013-0204
owncloud -- owncloud	Unspecified vulnerability in ownCloud Server before 4.0.12 allows remote attackers to obtain sensitive information via unspecified vectors related to "inclusion of the Amazon SDK testing suite." NOTE: due to lack of details, it is not clear whether the issue exists in ownCloud itself, or in Amazon SDK.	2014-06-05	5.0	CVE-2013-0302
owncloud -- owncloud	ownCloud Server before 4.5.7 does not properly check ownership of calendars, which allows remote authenticated users to read arbitrary calendars via the calid parameter to /apps/calendar/export.php. NOTE: this issue has been reported as a cross-site request forgery (CSRF) vulnerability, but due to lack of details, it is uncertain what the root cause is.	2014-06-05	4.0	CVE-2013-0304

owncloud -- owncloud	The installation routine in ownCloud Server before 4.0.14, 4.5.x before 4.5.9, and 5.0.x before 5.0.4 uses the time function to seed the generation of the PostgreSQL database user password, which makes it easier for remote attackers to guess the password via a brute force attack.	2014-06-04	5.0	CVE-2013-1941
owncloud -- owncloud	Cross-site scripting (XSS) vulnerability in the Documents component in ownCloud Server 6.0.x before 6.0.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly related to the print_unescaped function.	2014-06-04	4.3	CVE-2014-3832
owncloud -- owncloud	Multiple cross-site scripting (XSS) vulnerabilities in the (1) Gallery and (2) core components in ownCloud Server before 5.016 and 6.0.x before 6.0.3 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors, possibly related to the print_unescaped function.	2014-06-04	4.3	CVE-2014-3833
owncloud -- owncloud	ownCloud Server before 5.0.16 and 6.0.x before 6.0.3 does not check permissions to the files_external application, which allows remote authenticated users to add external storage via unspecified vectors.	2014-06-04	5.5	CVE-2014-3835
owncloud -- owncloud	Multiple cross-site request forgery (CSRF) vulnerabilities in ownCloud Server before 6.0.3 allow remote attackers to hijack the authentication of users for requests that (1) conduct cross-site scripting (XSS) attacks, (2) modify files, or (3) rename files via unspecified vectors.	2014-06-04	6.8	CVE-2014-3836
owncloud -- owncloud	The document application in ownCloud Server before 6.0.3 uses sequential values for the file_id, which allows remote authenticated users to enumerate shared files via unspecified vectors.	2014-06-04	4.0	CVE-2014-3837
owncloud -- owncloud	ownCloud Server before 5.0.16 and 6.0.x before 6.0.3 does not properly check permissions, which allows remote authenticated users to read the names of files of other users by leveraging access to multiple accounts.	2014-06-04	4.0	CVE-2014-3838

owncloud -- owncloud	ownCloud Server before 6.0.1 does not properly check permissions, which allows remote authenticated users to access arbitrary preview pictures via unspecified vectors.	2014-06-04	4.0	CVE-2014-3963
php -- php	The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.	2014-06-01	5.0	CVE-2014-0237
php -- php	The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.	2014-06-01	5.0	CVE-2014-0238
redhat -- openstack	The default configuration in the standalone controller quickstack manifest in openstack-foreman-installer, as used in Red Hat Enterprise Linux OpenStack Platform 4.0, disables authentication for Qpid, which allows remote attackers to gain access by connecting to Qpid.	2014-06-02	5.0	CVE-2013-6470
redhat -- openstack	OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, uses an HTTP connection to download (1) packages and (2) signing keys from Yum repositories, which allows man-in-the-middle attackers to prevent updates via unspecified vectors.	2014-06-02	4.3	CVE-2014-0040
redhat -- openstack	OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, sets sslverify to false for certain Yum repositories, which disables SSL protection and allows man-in-the-middle attackers to prevent updates via unspecified vectors.	2014-06-02	4.3	CVE-2014-0041
redhat -- openstack	OpenStack Heat Templates (heat-templates), as used in Red Hat Enterprise Linux OpenStack Platform 4.0, sets gpgcheck to 0 for certain templates, which disables GPG signature checking	2014-06-02	4.3	CVE-2014-0042

	on downloaded packages and allows man-in-the-middle attackers to install arbitrary packages via unspecified vectors.			
redhat -- sos	sosreport in Red Hat sos 1.7 and earlier on Red Hat Enterprise Linux (RHEL) 5 produces an archive with an fstab file 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.	2014-06-01	5.0	CVE-2014-3925
redhat -- enterprise_mrg	The Linux kernel through 3.14.5 does not properly consider the presence of hugetlb entries, which allows local users to cause a denial of service (memory corruption or system crash) by accessing certain memory locations, as demonstrated by triggering a race condition via numa_maps read operations during hugepage migration, related to fs/proc/task_mmu.c and mm/mempolicy.c.	2014-06-05	4.0	CVE-2014-3940
rom_walton -- boinc	Multiple stack-based buffer overflows in BOINC 6.13.x allow remote attackers to cause a denial of service (crash) via a long trickle-up to (1) client/cs_trickle.cpp or (2) db/db_base.cpp.	2014-06-02	5.0	CVE-2011-5280
rom_walton -- boinc	Format string vulnerability in the PROJECT::write_account_file function in client/cs_account.cpp in BOINC, possibly 7.2.33, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via format string specifiers in the gui_urls item in an account file.	2014-06-02	5.0	CVE-2013-7386
simple_popup_project -- simple_popup	Cross-site scripting (XSS) vulnerability in popup.php in the Simple Popup Images plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the z parameter.	2014-05-30	4.3	CVE-2014-3921
trend_micro -- interscan_messaging_security_virtual_appliance	Cross-site scripting (XSS) vulnerability in Trend Micro InterScan Messaging Security Virtual Appliance 8.5.1.1516 allows remote authenticated users to inject arbitrary web script or HTML via the	2014-05-30	4.3	CVE-2014-3922

	addWhiteListDomainStr parameter to addWhiteListDomain.imss.			
trianglemicroworks -- scada_data_gateway	Triangle MicroWorks SCADA Data Gateway before 3.00.0635 allows remote attackers to cause a denial of service (excessive data processing) via a crafted DNP3 packet.	2014-05-30	5.0	CVE-2014-2342
typo3 -- typo3	TYPO3 4.5.0 before 4.5.34, 4.7.0 before 4.7.19, 6.0.0 before 6.0.14, 6.1.0 before 6.1.9, and 6.2.0 before 6.2.3 allows remote attackers to have unspecified impact via a crafted HTTP Host header, related to "Host Spoofing."	2014-06-03	5.0	CVE-2014-3941
typo3 -- typo3	The Color Picker Wizard component in TYPO3 4.5.0 before 4.5.34, 4.7.0 before 4.7.19, 6.0.0 before 6.0.14, and 6.1.0 before 6.1.9 allows remote authenticated editors to execute arbitrary PHP code via a serialized PHP object.	2014-06-03	6.0	CVE-2014-3942
typo3 -- typo3	The Authentication component in TYPO3 6.2.0 before 6.2.3 does not properly invalidate timed out user sessions, which allows remote attackers to bypass authentication via unspecified vectors.	2014-06-03	5.8	CVE-2014-3944
typo3 -- typo3	The Authentication component in TYPO3 before 6.2, when salting for password hashing is disabled, does not require knowledge of the cleartext password if the password hash is known, which allows remote attackers to bypass authentication and gain access to the backend by leveraging knowledge of a password hash.	2014-06-03	4.0	CVE-2014-3945
typo3 -- typo3	The query caching functionality in the Extbase Framework component in TYPO3 6.2.0 before 6.2.3 does not properly validate group permissions, which allows remote authenticated users to read arbitrary queries via unspecified vectors.	2014-06-03	4.0	CVE-2014-3946
vmware -- fusion	VMware Tools in VMware Workstation 10.x before 10.0.2, VMware Player 6.x before 6.0.2, VMware Fusion 6.x before 6.0.3, and VMware ESXi 5.0 through 5.5, when a Windows 8.1 guest OS is used, allows guest OS users to gain guest OS privileges or cause a denial of service (kernel NULL pointer	2014-05-31	5.8	CVE-2014-3793

	dereference and guest OS crash) via unspecified vectors.			
webmin -- userwin	Multiple cross-site scripting (XSS) vulnerabilities in Webmin before 1.690 and Usermin before 1.600 allow remote attackers to inject arbitrary web script or HTML via vectors related to popup windows.	2014-05-30	4.3	CVE-2014-3924
xen -- xen	The HVMOP_inject_msi function in Xen 4.2.x, 4.3.x, and 4.4.x does not properly check the return value from the IRQ setup check, which allows local HVM guest administrators to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.	2014-06-05	5.5	CVE-2014-3967
xen -- xen	The HVMOP_inject_msi function in Xen 4.2.x, 4.3.x, and 4.4.x allows local guest HVM administrators to cause a denial of service (host crash) via a large number of crafted requests, which trigger an error messages to be logged.	2014-06-05	5.5	CVE-2014-3968
zemanta -- related_posts	Cross-site request forgery (CSRF) vulnerability in the Related Posts plugin before 2.7.2 for WordPress allows remote attackers to hijack the authentication of users for requests that modify settings via unspecified vectors.	2014-06-02	6.8	CVE-2013-3257
zemanta -- related_posts	Cross-site request forgery (CSRF) vulnerability in the WordPress Related Posts plugin before 2.6.2 for WordPress allows remote attackers to hijack the authentication of users for requests that change settings via unspecified vectors.	2014-06-02	6.8	CVE-2013-3476
znc -- znc	ZNC 1.0 allows remote authenticated users to cause a denial of service (NULL pointer reference and crash) via a crafted request to the (1) editnetwork, (2) editchan, (3) addchan, or (4) delchan page in modules/webadmin.cpp.	2014-06-05	4.0	CVE-2013-2130

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
david_bagley -- xlockmore	The (1) checkPasswd and (2) checkGroupXlockPasswds functions in xlockmore before 5.43 do not properly handle when a NULL value is returned upon an error by the crypt or dispcrypt function as implemented in glibc 2.17 and later, which allows attackers to bypass the screen lock via vectors related to invalid salts.	2014-05-30	2.1	CVE-2013-4143
ibm -- sterling_control_center	Open redirect vulnerability in IBM Sterling Control Center 5.4.0 before 5.4.0.1 iFix 3 and 5.4.1 before 5.4.1.0 iFix 2 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via a crafted URL.	2014-05-30	3.5	CVE-2014-0925
jo_hasenau -- gridelements	Cross-site scripting (XSS) vulnerability in the layout wizard in the Grid Elements (gridelements) extension before 1.5.1 and 2.0.x before 2.0.3 for TYPO3 allows remote authenticated backend users to inject arbitrary web script or HTML via unspecified vectors.	2014-06-04	3.5	CVE-2014-3949
mate-desktop -- mate-settings-daemon	The default configuration in mate-settings-daemon 1.5.3 allows local users to change the timezone for the system via a crafted D-Bus call.	2014-05-30	2.1	CVE-2012-5560
newsignature -- addressfield_tokens	Cross-site scripting (XSS) vulnerability in the address components field formatter in the AddressField Tokens module 7.x-1.x before 7.x-1.4 for Drupal allows remote authenticated users to inject arbitrary web script or HTML via an address field.	2014-06-02	3.5	CVE-2014-3933
redhat -- rhevm-dwh	The setup script in ovirt-engine-dwh, as used in the Red Hat Enterprise Virtualization Manager data warehouse (rhevm-dwh) package before 3.3.3, stores the history database password in cleartext,	2014-05-30	2.1	CVE-2014-0202

	which allows local users to obtain sensitive information by reading an unspecified file.			
redhat -- enterprise_mrg	kernel/auditsc.c in the Linux kernel through 3.14.5, when CONFIG_AUDITSYSCALL is enabled with certain syscall rules, allows local users to obtain potentially sensitive single-bit values from kernel memory or cause a denial of service (OOPS) via a large value of a syscall number.	2014-06-05	3.3	CVE-2014-3917
sendmail -- sendmail	The sm_close_on_exec function in conf.c in sendmail before 8.14.9 has arguments in the wrong order, and consequently skips setting expected FD_CLOEXEC flags, which allows local users to access unintended high-numbered file descriptors via a custom mail-delivery program.	2014-06-04	1.9	CVE-2014-3956
trianglemicroworks -- scada_data_gateway	Triangle MicroWorks SCADA Data Gateway before 3.00.0635 allows physically proximate attackers to cause a denial of service (excessive data processing) via a crafted DNP request over a serial line.	2014-05-30	2.1	CVE-2014-2343
typo3 -- typo3	Multiple cross-site scripting (XSS) vulnerabilities in unspecified backend components in TYPO3 4.5.0 before 4.5.34, 4.7.0 before 4.7.19, 6.0.0 before 6.0.14, 6.1.0 before 6.1.9, and 6.2.0 before 6.2.3 allow remote authenticated editors to inject arbitrary web script or HTML via unknown parameters.	2014-06-03	3.5	CVE-2014-3943

- 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).