UgCERT Computer Emergency Response Team

UCC UGANDA COMMUNICATIONS COMMISSION

Vulnerability Summary for the Week of May 26, 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
cisco -- nexus_7000	Cisco NX-OS 6.1 before 6.1(5) on Nexus 7000 devices, when local authentication and multiple VDCs are enabled, allows remote authenticated users to gain privileges within an unintended VDC via crafted SSH key data in an SSH session to a management interface, aka Bug ID CSCud88400.	2014-05-25	7.1	CVE-2013-1191
cisco -- wide_area_application_services	Cisco Wide Area Application Services (WAAS) 5.1.1 before 5.1.1e, when SharePoint prefetch optimization is enabled, allows remote SharePoint servers to execute arbitrary code via a malformed response, aka Bug ID CSCue18479.	2014-05-25	9.3	CVE-2014-2196
cisco -- nx-os	Cisco NX-OS 5.0 before 5.0(5) on Nexus 7000 devices, when local authentication and multiple VDCs are enabled, allows remote authenticated users to gain privileges within an unintended VDC via an SSH session to a management interface, aka Bug ID CSCti11629.	2014-05-25	7.1	CVE-2014-2200
cisco -- mds_9000	The Message Transfer Service (MTS) in Cisco NX-	2014-05-25	7.8	CVE-2014-2201

	OS before 6.2(7) on MDS 9000 devices and 6.0 before 6.0(2) on Nexus 7000 devices allows remote attackers to cause a denial of service (NULL pointer dereference and kernel panic) via a large volume of crafted traffic, aka Bug ID CSCtw98915.			
cisco -- cgr_1120	Buffer overflow in the Smart Call Home implementation in Cisco NX-OS on Fabric Interconnects in Cisco Unified Computing System 1.4 before 1.4(1i), NX-OS 5.0 before 5.0(3)U2(2) on Nexus 3000 devices, NX-OS 4.1 before 4.1(2)E1(1l) on Nexus 4000 devices, NX-OS 5.x before 5.1(3)N1(1) on Nexus 5000 devices, NX-OS 5.2 before 5.2(3a) on Nexus 7000 devices, and CG-OS CG4 before CG4(2) on Connected 1000 Connected Grid Routers allows remote SMTP servers to execute arbitrary code via a crafted reply, aka Bug IDs CSCtk00695, CSCts56633, CSCts56632, CSCts56628, CSCug14405, and CSCuf61322.	2014-05-25	7.6	CVE-2014-3261
citrix -- cloudplatform	Citrix CloudPlatform (formerly Citrix CloudStack) 3.0.x before 3.0.6 Patch C does not properly restrict access to VNC ports on the management network, which allows remote attackers to have unspecified impact via unknown vectors.	2014-05-23	7.5	CVE-2013-2757
coscms -- coscms	The uploadFile function in upload/index.php in CosCMS before 1.822 allows remote administrators to execute arbitrary commands via shell metacharacters in the name of an uploaded file.	2014-05-23	8.5	CVE-2013-1668
d-link -- dap-1350	Multiple SQL injection vulnerabilities in the administration login page in D-Link DAP-1350 (Rev. A1) with firmware 1.14 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) username or (2) password.	2014-05-27	7.5	CVE-2014-3872
emc -- documentum_d2	EMC Documentum D2 3.1 before P20, 3.1 SP1 before P02, 4.0 before P10, 4.1 before P13, and 4.2 before P01 allows remote authenticated	2014-05-25	9.0	CVE-2014-2504

	users to bypass intended access restrictions and execute arbitrary Documentum Query Language (DQL) queries by calling (1) a core method or (2) a D2FS web-service method.			
geodesicsolutions -- geocore_max	Multiple SQL injection vulnerabilities in register.php in Geodesic Solutions GeoCore MAX 7.3.3 (formerly GeoClassifieds and GeoAuctions) allow remote attackers to execute arbitrary SQL commands via the (1) c[password] or (2) c[username] parameter. NOTE: the b parameter to index.php vector is already covered by CVE-2006-3823.	2014-05-27	7.5	CVE-2014-3871
hp -- operations_manager_i	Unspecified vulnerability in HP Operations Manager i 9.1 through 9.13 and 9.2 through 9.24 allows remote authenticated users to execute arbitrary code by leveraging the OMi operator role.	2014-05-25	8.5	CVE-2014-2607
ibm -- websphere_commerce	IBM WebSphere Commerce 6.0 Feature Pack 2 through Feature Pack 5, 7.0.0.0 through 7.0.0.8, and 7.0 Feature Pack 1 through Feature Pack 7 allows remote attackers to cause a denial of service (resource consumption and daemon crash) via a malformed id parameter in a request.	2014-05-25	7.1	CVE-2014-0943
pandasecurity -- panda_av_pro_2014	Unspecified vulnerability in Panda Gold Protection and Global Protection 2014 7.01.01 and earlier, Internet Security 2014 19.01.01 and earlier, and AV Pro 2014 13.01.01 and earlier allows local users to gain privileges via unspecified vectors.	2014-05-23	7.2	CVE-2014-3450
squash -- square_squash	The Square Squash allows remote attackers to execute arbitrary code via a YAML document in the (1) namespace parameter to the deobfuscation function or (2) sourcemap parameter to the sourcemap function in app/controllers/api/v1_controller.rb.	2014-05-27	7.5	CVE-2013-5036
uplawski -- creme_fraiche	The set_meta_data function in lib/cremefraiche.rb in the Creme Fraiche gem before 0.6.1 for Ruby allows remote attackers to	2014-05-27	9.3	CVE-2013-2090

	execute arbitrary commands via shell metacharacters in the file name of an email attachment. NOTE: some of these details are obtained from third party information.			
wpshopstyling -- wp-ecommerce-shop-styling	PHP remote file inclusion vulnerability in includes/generate-pdf.php in the WP ecommerce Shop Styling plugin for WordPress before 1.8 allows remote attackers to execute arbitrary PHP code via a URL in the dompdf parameter.	2014-05-27	7.5	CVE-2013-0724

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
apache -- couchdb	Apache CouchDB before 1.0.4, 1.1.x before 1.1.2, and 1.2.x before 1.2.1 allows remote attackers to execute arbitrary code via a JSONP callback, related to Adobe Flash.	2014-05-23	6.8	CVE-2012-5649
apache -- hbase	Apache HBase 0.92.x before 0.92.3 and 0.94.x before 0.94.9, when the Kerberos features are enabled, allows man-in-the-middle attackers to disable bidirectional authentication and obtain sensitive information via unspecified vectors.	2014-05-29	4.3	CVE-2013-2193
apache -- cloudstack	Apache CloudStack 4.0.0 before 4.0.2 and Citrix CloudPlatform (formerly Citrix CloudStack) 3.0.x before 3.0.6 Patch C allows remote attackers to bypass the console proxy authentication by leveraging knowledge of the source code.	2014-05-23	5.0	CVE-2013-2756

apache -- cloudstack	Apache CloudStack 4.0.0 before 4.0.2 and Citrix CloudPlatform (formerly Citrix CloudStack) 3.0.x before 3.0.6 Patch C uses a hash of a predictable sequence, which makes it easier for remote attackers to guess the console access URL via a brute force attack.	2014-05-23	5.0	CVE-2013-2758
axway -- email_firewall	Axway Secure Messenger before 6.5 Updated Release 7, as used in Axway Email Firewall, provides different responses to authentication requests depending on whether the user exists, which allows remote attackers to enumerate users via a series of requests.	2014-05-27	5.0	CVE-2012-6452
bib2html_project -- bib2html	Cross-site scripting (XSS) vulnerability in the bib2html plugin 0.9.3 for WordPress allows remote attackers to inject arbitrary web script or HTML via the styleShortName parameter in an adminStyleAdd action to OSBiB/create/index.php.	2014-05-27	4.3	CVE-2014-3870
cisco -- security_manager	Cross-site scripting (XSS) vulnerability in the web framework in Cisco Security Manager 4.6 and earlier allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka Bug ID CSCun65189.	2014-05-25	4.3	CVE-2014-3266
cisco -- security_manager	Cross-site request forgery (CSRF) vulnerability in the web framework in Cisco Security Manager 4.6 and earlier allows remote attackers to hijack the authentication of arbitrary users for requests that make unspecified changes, aka Bug ID CSCuo46427.	2014-05-25	6.8	CVE-2014-3267
cisco -- tidal_enterprise_scheduler	The Agent in Cisco Tidal Enterprise Scheduler (TES) 6.1 and earlier allows local users to gain privileges via crafted Tidal Job Buffers (TJB) parameters, aka Bug ID CSCuo33074.	2014-05-25	6.0	CVE-2014-3272
cisco -- telepresence_system_software	Cisco TelePresence System (CTS) 6.0(.5)(5) and earlier falls back to HTTP when certain HTTPS sessions cannot be established, which allows man-in-the-middle attackers to obtain sensitive directory information by leveraging a network position between CTS and Cisco Unified Communications Manager (UCM) to block HTTPS traffic, aka Bug ID	2014-05-25	4.3	CVE-2014-3274

	CSCuj26326.			
cisco -- identity_services_engine_software	SQL injection vulnerability in the web framework in Cisco Identity Services Engine (ISE) 1.2(.1 patch 2) and earlier allows remote authenticated users to execute arbitrary SQL commands via a crafted URL, aka Bug ID CSCul21337.	2014-05-25	6.5	CVE-2014-3275
cisco -- identity_services_engine_software	Cisco Identity Services Engine (ISE) 1.2(.1 patch 2) and earlier does not properly handle deadlock conditions during reception of crafted RADIUS accounting packets from multiple NAS devices, which allows remote authenticated users to cause a denial of service (RADIUS outage) by sourcing these packets from two origins, aka Bug ID CSCuo56780.	2014-05-25	4.0	CVE-2014-3276
cisco -- unified_communications_domain_manager	The Administration GUI in 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 sensitive user and group information by leveraging Location Administrator privileges and entering a crafted URL, aka Bug ID CSCum77005.	2014-05-29	4.0	CVE-2014-3277
cisco -- unified_communications_domain_manager	The Administration GUI in 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 attackers to enumerate account names via a crafted URL, aka Bug IDs CSCun39631 and CSCun39643.	2014-05-29	5.0	CVE-2014-3279
cisco -- unified_communications_domain_manager	The Administration GUI in 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 sensitive number-translation information by leveraging Location Administrator privileges and entering a crafted URL, aka Bug ID CSCum76930.	2014-05-29	4.0	CVE-2014-3282
cisco -- unified_communications_domain_man	Open redirect vulnerability in Self-Care Client Portal applications in the web framework in VOSS in Cisco Unified Communications Domain Manager (CDM)	2014-05-29	5.8	CVE-2014-3283

ager	9.0(.1) and earlier allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a crafted URL, aka Bug ID CSCun79731.			
cisco -- asr_1001_router	Cisco IOS XE on ASR1000 devices, when PPPoE termination is enabled, allows remote attackers to cause a denial of service (device reload) via a malformed PPPoE packet, aka Bug ID CSCuo55180.	2014-05-25	6.1	CVE-2014-3284
cisco -- wide_area_application_services	Cisco Wide Area Application Services (WAAS) 5.3(.5a) and earlier, when SharePoint acceleration is enabled, does not properly parse SharePoint responses, which allows remote attackers to cause a denial of service (application-optimization handler reload) via a crafted SharePoint application, aka Bug ID CSCue47674.	2014-05-29	5.0	CVE-2014-3285
davistribe -- google_doc_embedder	Directory traversal vulnerability in the Google Doc Embedder plugin before 2.5.4 for WordPress allows remote attackers to read arbitrary files via a .. (dot dot) in the file parameter to libs/pdf.php.	2014-05-29	5.0	CVE-2012-4915
dovecot -- dovecot	The IMAP functionality in Dovecot before 2.2.2 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via invalid APPEND parameters.	2014-05-27	5.0	CVE-2013-2111
ekiga -- ekiga	The Portable Tool Library (aka PTLib) before 2.10.10, as used in Ekiga before 4.0.1, does not properly detect recursion during entity expansion, which allows remote attackers to cause a denial of service (memory and CPU consumption) via a crafted PXML document containing a large number of nested entity references, aka a "billion laughs attack."	2014-05-23	4.3	CVE-2013-1864
emc -- rsa_archer_egrc	Multiple cross-site scripting (XSS) vulnerabilities in EMC RSA Archer 5.x before GRC 5.4 SP1 P3 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-25	4.3	CVE-2014-0639
gentoo -- nullmailer	The Gentoo Nullmailer package before 1.11-r2 uses world-readable permissions for /etc/nullmailer/remotes, which allows local users to obtain SMTP authentication credentials by reading	2014-05-23	5.0	CVE-2013-4223

	the file.			
glpi-project -- glpi	inc/ticket.class.php in GLPI 0.83.9 and earlier allows remote attackers to unserialize arbitrary PHP objects via the _predefined_fields parameter to front/ticket.form.php.	2014-05-27	6.4	CVE-2013-2225
google_authenticator_login_project -- ga_login	The Google Authenticator login module 6.x-1.x before 6.x-1.2 and 7.x-1.x before 7.x-1.4 for Drupal does not properly identify user account names, which might allow remote attackers to bypass the two-factor authentication requirement via unspecified vectors.	2014-05-29	5.0	CVE-2013-4177
google_authenticator_login_project -- ga_login	The Google Authenticator login module 6.x-1.x before 6.x-1.2 and 7.x-1.x before 7.x-1.4 for Drupal allows remote attackers to obtain access by replaying the username, password, and one-time password (OTP).	2014-05-29	5.0	CVE-2013-4178
groups,_communities_and_co_project -- gcc	The Groups, Communities and Co (GCC) module 7.x-1.x before 7.x-1.1 for Drupal does not properly check permission, which allows remote attackers to access the configuration pages via unspecified vectors.	2014-05-27	5.0	CVE-2013-4598
ibm -- maximo_asset_management	CRLF injection vulnerability in IBM Maximo Asset Management 7.x before 7.5.0.6 and SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a crafted parameter in a URL.	2014-05-26	4.3	CVE-2012-3333
ibm -- sametime	Unspecified vulnerability in the Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote attackers to discover user names, full names, and e-mail addresses via a search.	2014-05-26	5.0	CVE-2013-3975
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote attackers to determine which meeting rooms are owned by a user by leveraging knowledge of valid user names.	2014-05-26	4.3	CVE-2013-3977

ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote attackers to cause a denial of service (room unusability) by generating a large number of fictitious users to enter a meeting room.	2014-05-26	5.0	CVE-2013-3980
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote attackers to download avatar photos of arbitrary users via unspecified vectors.	2014-05-26	5.0	CVE-2013-3981
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote attackers to obtain unspecified installation information and technical data via a request to a public page.	2014-05-26	5.0	CVE-2013-3982
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 does not set the secure flag for an unspecified cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2014-05-26	5.0	CVE-2013-3984
ibm -- change_and_configuration_management_database	SQL injection vulnerability in IBM Maximo Asset Management 7.x before 7.1.1.7 LAFIX.20140319-0837, 7.1.1.11 before IFIX.20140323-0749, 7.1.1.12 before IFIX.20140321-1336, 7.5.x before 7.5.0.3 IFIX027, 7.5.0.4 before IFIX011, and 7.5.0.5 before IFIX006; SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2; and Tivoli IT Asset Management for IT, Tivoli Service Request Manager, Maximo Service Desk, and Change and Configuration Management Database (CCMDB) 7.x before 7.1.1.7 LAFIX.20140319-0837, 7.1.1.11 before IFIX.20140207-1801, and 7.1.1.12 before IFIX.20140218-1510 allows remote authenticated users to execute arbitrary SQL commands via a Birt report with a WHERE clause in plain text.	2014-05-26	6.5	CVE-2013-4016
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.5.x before 7.5.0.3 IFIX027, 7.5.0.4 before IFIX011, and 7.5.0.5 before IFIX006 and SmartCloud Control Desk 7.x before	2014-05-26	6.0	CVE-2013-5464

	7.5.0.3 and 7.5.1.x before 7.5.1.2 allow remote authenticated users to bypass intended access restrictions, and modify physical counts associated with restricted storerooms, via unspecified vectors.			
ibm -- change_and_configuration_management_database	IBM Maximo Asset Management 7.x before 7.1.1.7 LAFIX.20140319-0837, 7.1.1.11 before IFIX.20140323-0749, 7.1.1.12 before IFIX.20140321-1336, 7.5.x before 7.5.0.3 IFIX027, and 7.5.0.4 before IFIX011; SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2; and Tivoli IT Asset Management for IT, Tivoli Service Request Manager, Maximo Service Desk, and Change and Configuration Management Database (CCMDB) 7.x before 7.1.1.7 LAFIX.20140319-0837, 7.1.1.11 before IFIX.20140207-1801, and 7.1.1.12 before IFIX.20140218-1510 do not properly restrict file types during uploads, which allows remote authenticated users to have an unspecified impact via an invalid type.	2014-05-26	6.5	CVE-2013-5465
ibm -- tivoli_storage_manager_for_virtual_environments	The Data Protection for VMware component in IBM Tivoli Storage Manager for Virtual Environments (TSMVE) 6.3 through 7.1.0.2 does not properly check authorization for backup and restore operations, which allows local users to obtain sensitive VM data or cause a denial of service (disk consumption) via unspecified GUI actions.	2014-05-26	4.1	CVE-2013-6713
ibm -- tivoli_storage_flashcopy_manager	The FlashCopy Manager for VMware component in IBM Tivoli Storage FlashCopy Manager 3.1 through 4.1.0.1 does not properly check authorization for backup and restore operations, which allows local users to obtain sensitive VM data or cause a denial of service (data overwrite or disk consumption) via unspecified GUI actions.	2014-05-26	4.1	CVE-2013-6714
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.x before 7.5.0.3 IFIX027 and SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2 allow remote authenticated users to gain privileges by leveraging membership in two security groups.	2014-05-26	6.0	CVE-2014-0849

ibm -- java_sdk	The IBMSecureRandom component in the IBMJCE and IBMSecureRandom cryptographic providers in IBM SDK Java Technology Edition 5.0 before Service Refresh 16 FP6, 6 before Service Refresh 16, 6.0.1 before Service Refresh 8, 7 before Service Refresh 7, and 7R1 before Service Refresh 1 makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms by predicting the random number generator's output.	2014-05-26	5.8	CVE-2014-0878
ibm -- maximo_asset_management	Cross-site scripting (XSS) vulnerability in customreport.jsp in IBM Maximo Asset Management 7.5.x before 7.5.0.5 IFIX006 and SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2 allows remote authenticated users to inject arbitrary web script or HTML via unspecified parameters.	2014-05-26	4.3	CVE-2014-0893
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 does not check whether a session cookie is current, which allows remote attackers to conduct user-search actions by leveraging possession of a (1) expired or (2) invalidated cookie.	2014-05-26	4.3	CVE-2014-0906
ibm -- sametime	Cross-site scripting (XSS) vulnerability in the Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL.	2014-05-26	4.3	CVE-2014-3014
ibm -- sametime_proxy_server_and_web_client	Cross-site request forgery (CSRF) vulnerability in the Web player in IBM Sametime Proxy Server and Web Client 9.0 through 9.0.0.1 allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences.	2014-05-25	6.8	CVE-2014-3015
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 does not include the HTTPOnly flag in a Set-Cookie header for an unspecified cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie, a	2014-05-26	5.0	CVE-2014-3867

	different vulnerability than CVE-2013-3984.			
imember360 -- imember360	The iMember360 plugin before 3.9.001 for WordPress does not properly restrict access, which allows remote attackers to obtain database credentials via the i4w_dbinfo parameter.	2014-05-23	5.0	CVE-2014-3848
imember360 -- imember360	The iMember360 plugin 3.8.012 through 3.9.001 for WordPress does not properly restrict access, which allows remote attackers to delete arbitrary users via a request containing a user name in the Email parameter and the API key in the i4w_clearuser parameter.	2014-05-23	4.3	CVE-2014-3849
izarc -- izarc	IZArc 4.1.8 displays a file's name on the basis of a ZIP archive's Central Directory entry, but launches this file on the basis of a ZIP archive's local file header, which allows user-assisted remote attackers to conduct file-extension spoofing attacks via a modified Central Directory, as demonstrated by unintended code execution prompted by a .jpg extension in the Central Directory and a .exe extension in the local file header.	2014-05-27	6.8	CVE-2014-2720
jasig -- uportal	uPortal before 4.0.13.1 does not properly check the MANAGE permissions, which allows remote authenticated users to manage arbitrary portlets by leveraging the SUBSCRIBE permission for the portlet-admin portlet.	2014-05-29	6.5	CVE-2014-3416
jasig -- uportal	uPortal before 4.0.13.1 does not properly check the CONFIG permission, which allows remote authenticated users to configure portlets by leveraging the SUBSCRIBE permission for a portlet.	2014-05-29	6.5	CVE-2014-3417
kieranoshea -- calendar	Cross-site request forgery (CSRF) vulnerability in the Calendar plugin before 1.3.3 for WordPress allows remote attackers to hijack the authentication of users for requests that add a calendar entry via unspecified vectors.	2014-05-27	6.8	CVE-2013-2698
krisonav -- krisonav	Cross-site scripting (XSS) vulnerability in services/get_article.php in KrisonAV CMS before 3.0.2 allows remote attackers to inject arbitrary web script or HTML via the content parameter.	2014-05-23	4.3	CVE-2013-2712

krisonav -- krisonav	Cross-site request forgery (CSRF) vulnerability in users_maint.html in KrisonAV CMS before 3.0.2 allows remote attackers to hijack the authentication of administrators for requests that create user accounts via a crafted request.	2014-05-23	6.8	CVE-2013-2713
libguestfs -- libguestfs	Double free vulnerability in inspect-fs.c in LibguestFS 1.20.x before 1.20.7, 1.21.x, 1.22.0, and 1.23.0 allows remote attackers to cause a denial of service (crash) via empty guest files.	2014-05-27	4.3	CVE-2013-2124
linux -- linux_kernel	The futex_wait_requeue_pi function in kernel/futex.c in the Linux kernel before 3.5.1 does not ensure that calls have two different futex addresses, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted FUTEX_WAIT_REQUEUE_PI command.	2014-05-26	4.9	CVE-2012-6647
mantisbt -- mantisbt	Mantis Bug Tracker (aka MantisBT) 1.2.12 before 1.2.15 allows remote attackers to cause a denial of service (resource consumption) via a filter using a criteria, text search, and the "any condition" match type.	2014-05-27	5.0	CVE-2013-1883
modwsgi -- mod_wsgi	The mod_wsgi module before 3.5 for Apache, when daemon mode is enabled, does not properly handle error codes returned by setuid when run on certain Linux kernels, which allows local users to gain privileges via vectors related to the number of running processes.	2014-05-27	6.2	CVE-2014-0240
moodle -- moodle	Multiple cross-site request forgery (CSRF) vulnerabilities in mod/assign/locallib.php in the Assignment subsystem in Moodle through 2.3.11, 2.4.x before 2.4.10, 2.5.x before 2.5.6, and 2.6.x before 2.6.3 allow remote attackers to hijack the authentication of teachers for quick-grading requests.	2014-05-26	6.8	CVE-2014-0213
moodle -- moodle	login/token.php in Moodle through 2.3.11, 2.4.x before 2.4.10, 2.5.x before 2.5.6, and 2.6.x before 2.6.3 creates a MoodleMobile web-service token with an infinite lifetime, which makes it easier for	2014-05-26	6.8	CVE-2014-0214

	remote attackers to hijack sessions via a brute-force attack.			
moodle -- moodle	The blind-marking implementation in Moodle through 2.3.11, 2.4.x before 2.4.10, 2.5.x before 2.5.6, and 2.6.x before 2.6.3 allows remote authenticated users to de-anonymize student identities by (1) using a screen reader or (2) reading the HTML source.	2014-05-26	4.0	CVE-2014-0215
moodle -- moodle	The My Home implementation in the block_html_pluginfile function in blocks/html/lib.php in Moodle through 2.3.11, 2.4.x before 2.4.10, 2.5.x before 2.5.6, and 2.6.x before 2.6.3 does not properly restrict file access, which allows remote attackers to obtain sensitive information by visiting an HTML block.	2014-05-26	5.0	CVE-2014-0216
moodle -- moodle	enrol/index.php in Moodle 2.6.x before 2.6.3 does not check for the moodle/course:viewhiddencourses capability before listing hidden courses, which allows remote attackers to obtain sensitive name and summary information about these courses by leveraging the guest role and visiting a crafted URL.	2014-05-26	4.3	CVE-2014-0217
moodle -- moodle	Cross-site scripting (XSS) vulnerability in the URL downloader repository in repository/url/lib.php in Moodle through 2.3.11, 2.4.x before 2.4.10, 2.5.x before 2.5.6, and 2.6.x before 2.6.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-26	4.3	CVE-2014-0218
nullsoft -- winamp	Winamp 5.666 and earlier allows remote attackers to cause a denial of service (memory corruption and crash) via a malformed .FLV file, related to f263.w5s.	2014-05-23	4.3	CVE-2014-3442
openbsd -- opensmtpd	OpenSMTPD before 5.3.2 does not properly handle SSL sessions, which allows remote attackers to cause a denial of service (connection blocking) by keeping a connection open.	2014-05-27	5.0	CVE-2013-2125
oswald_buddenhagen -- isync	Isync 0.4 before 1.0.6, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the	2014-05-23	4.3	CVE-2013-0289

	X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.			
paul_mattes -- x3270	x3270 before 3.3.12ga12 does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.	2014-05-27	5.8	CVE-2012-5662
redhat -- freeipa	The default LDAP ACIs in FreeIPA 3.0 before 3.1.2 do not restrict access to the (1) ipaNTTrustAuthIncoming and (2) ipaNTTrustAuthOutgoing attributes, which allow remote attackers to obtain the Cross-Realm Kerberos Trust key via unspecified vectors.	2014-05-29	5.0	CVE-2013-0199
samba -- samba	The internal DNS server in Samba 4.x before 4.0.18 does not check the QR field in the header section of an incoming DNS message before sending a response, which allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged response packet that triggers a communication loop, a related issue to CVE-1999-0103.	2014-05-28	5.0	CVE-2014-0239
sharetronix -- sharetronix	Cross-site request forgery (CSRF) vulnerability in Sharetronix before 3.4 allows remote attackers to hijack the authentication of administrators for requests that add administrative privileges to a user via the admin parameter to admin/administrators.	2014-05-29	6.8	CVE-2014-3414
sharetronix -- sharetronix	SQL injection vulnerability in Sharetronix before 3.4 allows remote authenticated users to execute arbitrary SQL commands via the invite_users[] parameter to the /invite page for a group.	2014-05-29	6.5	CVE-2014-3415
sosreport_project -- sosreport	SOSreport stores the md5 hash of the GRUB bootloader password in an archive, which allows local users to obtain sensitive information by reading the archive.	2014-05-29	4.3	CVE-2014-0246
usercake -- usercake	Multiple cross-site request forgery (CSRF) vulnerabilities in user_settings.php in Usercake	2014-05-26	6.8	CVE-2014-3866

	2.0.2 and earlier allow remote attackers to hijack the authentication of administrators for requests that change the (1) administrative password via the passwordc parameter or (2) administrative e-mail address via the email parameter.			
zemanta -- related_posts	Cross-site request forgery (CSRF) vulnerability in the Related Posts by Zemanta plugin before 1.3.2 for WordPress allows remote attackers to hijack the authentication of unspecified users for requests that change settings via unknown vectors.	2014-05-27	6.8	CVE-2013-3477

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
hub_project -- hub	The am function in lib/hub/commands.rb in hub before 1.12.1 allows local users to overwrite arbitrary files via a symlink attack on a temporary patch file.	2014-05-27	3.6	CVE-2014-0177
ibm -- maximo_asset_management	frontcontroller.jsp in IBM Maximo Asset Management 7.x before 7.5.0.6 and SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2 allows remote authenticated users to obtain sensitive information via an invalid action_code.	2014-05-26	3.5	CVE-2013-2998
ibm -- sametime	The Meeting Server in IBM Sametime 8.x through 8.5.2.1 and 9.x through 9.0.0.1 does not send the HSTS Strict-Transport-Security header, which makes it easier for man-in-the-middle attackers to hijack sessions or obtain sensitive information by leveraging the presence of HTTP requests.	2014-05-26	2.9	CVE-2013-3046

ibm -- maximo_asset_management	IBM Maximo Asset Management 7.x before 7.5.0.6 and SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2 allow remote authenticated users to bypass intended access restrictions, and read communication logs associated with unrelated records, via unspecified vectors.	2014-05-26	3.5	CVE-2013-5460
ibm -- change_and_configuration_management_database	IBM Maximo Asset Management 7.x before 7.1.1.7 LAFIX.20140319-0837 and 7.5.x before 7.5.0.5 IFIX006; SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2; and Tivoli IT Asset Management for IT, Tivoli Service Request Manager, Maximo Service Desk, and Change and Configuration Management Database (CCMDB) 7.x before 7.1.1.7 LAFIX.20140319-0837 allow remote authenticated users to obtain potentially sensitive stack-trace information by triggering a Birt error.	2014-05-26	3.5	CVE-2013-6741
ibm -- change_and_configuration_management_database	Cross-site scripting (XSS) vulnerability in IBM Maximo Asset Management 7.x before 7.1.1.8 LAFIX.20140319-0839 and 7.1.1.12 before IFIX.20140321-1336 and Tivoli IT Asset Management for IT, Tivoli Service Request Manager, Maximo Service Desk, and Change and Configuration Management Database (CCMDB) 7.x before 7.1.1.8 LAFIX.20140319-0839 and 7.1.1.12 before IFIX.20140218-1510 allows remote authenticated users to inject arbitrary web script or HTML via an attachment URL.	2014-05-26	3.5	CVE-2014-0824
ibm -- change_and_configuration_management_database	Cross-site scripting (XSS) vulnerability in openreport.jsp in IBM Maximo Asset Management 7.x before 7.1.1.12 IFIX.20140321-1336 and 7.5.x before 7.5.0.5 IFIX006; SmartCloud Control Desk 7.x before 7.5.0.3 and 7.5.1.x before 7.5.1.2; and Tivoli IT Asset Management for IT, Tivoli Service Request Manager, Maximo Service Desk, and Change and Configuration Management Database (CCMDB) 7.x before 7.1.1.12 IFIX.20140218-1510 allows remote authenticated users to inject arbitrary web script or HTML via a crafted report parameter.	2014-05-26	3.5	CVE-2014-0825
mayan-edms --	Multiple cross-site scripting (XSS) vulnerabilities in	2014-05-27	3.5	CVE-2014-3840

mayan_edms	apps/common/templates/calculate_form_title.html in Mayan EDMS 0.13 allow remote authenticated users to inject arbitrary web script or HTML via a (1) tag or the (2) title of a source in a Staging folder, (3) Name field in a bootstrap setup, or Title field in a (4) smart link or (5) web form.			
openstack -- heat	OpenStack Orchestration API (Heat) 2013.2 through 2013.2.3 and 2014.1, when creating the stack for a template using a provider template, allows remote authenticated users to obtain the provider template URL via the resource-type-list.	2014-05-23	3.5	CVE-2014-3801
redhat -- rhevm-reports	The setup script in ovirt-engine-reports, as used in the Red Hat Enterprise Virtualization reports (rhevm-reports) package before 3.3.3, stores the reports database password in cleartext, which allows local users to obtain sensitive information by reading an unspecified file.	2014-05-29	2.1	CVE-2014-0199
redhat -- rhevm-reports	The Red Hat Enterprise Virtualization Manager reports (rhevm-reports) package before 3.3.3-1 uses world-readable permissions on the datasource configuration file (js-jboss7-ds.xml), which allows local users to obtain sensitive information by reading the file.	2014-05-29	2.1	CVE-2014-0200
redhat -- rhevm-reports	ovirt-engine-reports, as used in the Red Hat Enterprise Virtualization reports package (rhevm-reports) before 3.3.3, uses world-readable permissions on configuration files, which allows local users to obtain sensitive information by reading the files.	2014-05-29	2.1	CVE-2014-0201
samba -- samba	Samba 3.6.6 through 3.6.23, 4.0.x before 4.0.18, and 4.1.x before 4.1.8, when a certain vfs shadow copy configuration is enabled, does not properly initialize the SRV_SNAPSHOT_ARRAY response field, which allows remote authenticated users to obtain potentially sensitive information from process memory via a (1) FSCTL_GET_SHADOW_COPY_DATA or (2) FSCTL_SRV_ENUMERATE_SNAPSHOTS request.	2014-05-28	3.5	CVE-2014-0178

- 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