Vulnerability Summary for the Week of May 12, 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**
adaptivecomputing -- torque_resource_manager	Stack-based buffer overflow in lib/Libdis/disrsi_.c in Terascale Open-Source Resource and Queue Manager (aka TORQUE Resource Manager) 2.5.x through 2.5.13 allows remote attackers to execute arbitrary code via a large count value.	2014-05-16	10.0	CVE-2014-0749
adobe -- illustrator	Stack-based buffer overflow in Adobe Illustrator CS6 before 16.0.5 and 16.2.x before 16.2.2 allows remote attackers to execute arbitrary code via unspecified vectors.	2014-05-14	10.0	CVE-2014-0513
adobe -- adobe_air	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow remote attackers to bypass the Same Origin Policy via unspecified vectors.	2014-05-14	7.5	CVE-2014-0516
adobe -- adobe_air	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111	2014-05-14	7.5	CVE-2014-0517

	allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0518, CVE-2014-0519, and CVE-2014-0520.			
adobe -- adobe_air	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0519, and CVE-2014-0520.	2014-05-14	7.5	CVE-2014-0518
adobe -- adobe_air	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0520.	2014-05-14	7.5	CVE-2014-0519
adobe -- adobe_air	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0519.	2014-05-14	7.5	CVE-2014-0520
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0523, CVE-2014-0524, and CVE-2014-0526.	2014-05-14	10.0	CVE-2014-0522
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allow attackers to execute arbitrary code or	2014-05-14	10.0	CVE-2014-0523

	cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0522, CVE-2014-0524, and CVE-2014-0526.			
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0522, CVE-2014-0523, and CVE-2014-0526.	2014-05-14	10.0	CVE-2014-0524
adobe -- acrobat	The API in Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X does not prevent access to unmapped memory, which allows attackers to execute arbitrary code via unspecified API calls.	2014-05-14	10.0	CVE-2014-0525
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0522, CVE-2014-0523, and CVE-2014-0524.	2014-05-14	10.0	CVE-2014-0526
adobe -- acrobat	Use-after-free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	2014-05-14	10.0	CVE-2014-0527
adobe -- acrobat	Double free vulnerability in Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	2014-05-14	10.0	CVE-2014-0528
adobe -- acrobat	Buffer overflow in Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors.	2014-05-14	10.0	CVE-2014-0529
broadcom -- pipa_c211_web_interface	cgi-bin/rpcBridge in the web interface 1.1 on Broadcom Ltd PIPA C211 rev2 does not properly restrict access, which allows remote attackers to	2014-05-13	9.7	CVE-2014-2046

	(1) obtain credentials and other sensitive information via a certain request to the config.getValuesHashExcludePaths method or (2) modify the firmware via unspecified vectors.			
d-link -- dir-505l_shareport_mobile_companion	D-Link DIR-505L SharePort Mobile Companion 1.01 and DIR-826L Wireless N600 Cloud Router 1.02 allows remote attackers to bypass authentication via a direct request when an authorized session is active.	2014-05-12	9.3	CVE-2013-4772
debian -- dpkg	dpkg 1.17.x before 1.17.9, 1.16.x before 1.16.14, and 1.15.x before 1.15.10 for Debian squeeze and wheezy supports "C-style encoded filenames" while the patch program does not, which introduces an interaction error that allows attackers to conduct directory traversal attacks and create files outside of the intended directories via a crafted package. NOTE: this vulnerability exists because of an incorrect fix for CVE-2014-0471.	2014-05-13	7.1	CVE-2014-3127
disk_pool_manager_project -- disk_pool_manager	Multiple SQL injection vulnerabilities in LCG Disk Pool Manager (DPM) before 1.8.6, as used in EGI UDM, allow remote attackers to execute arbitrary SQL commands via the (1) r_token variable in the dpm_get_pending_req_by_token, (2) dpm_get_cpr_by_fullid, (3) dpm_get_cpr_by_surl, (4) dpm_get_cpr_by_surls, (5) dpm_get_gfr_by_fullid, (6) dpm_get_gfr_by_surl, (7) dpm_get_pfr_by_fullid, (8) dpm_get_pfr_by_surl, (9) dpm_get_req_by_token, (10) dpm_insert_cpr_entry, (11) dpm_insert_gfr_entry, (12) dpm_insert_pending_entry, (13) dpm_insert_pfr_entry, (14) dpm_insert_xferreq_entry, (15) dpm_list_cpr_entry, (16) dpm_list_gfr_entry, or	2014-05-13	7.5	CVE-2011-4970

	(17) dpm_list_pfr_entry function; the (18) surl variable in the dpm_get_cpr_by_surl function; the (19) to_surl variable in the dpm_get_cpr_by_surls function; the (20) u_token variable in the dpm_get_pending_reqs_by_u_desc, (21) dpm_get_reqs_by_u_desc, (22) dpm_get_spcmd_by_u_desc, (23) dpm_insert_pending_entry, (24) dpm_insert_spcmd_entry, or (25) dpm_insert_xferreq_entry function; the (26) s_token variable in the dpm_get_spcmd_by_token, (27) dpm_insert_cpr_entry, (28) dpm_insert_gfr_entry, (29) dpm_insert_pfr_entry, (30) dpm_insert_spcmd_entry, (31) dpm_update_cpr_entry, (32) dpm_update_gfr_entry, or (33) dpm_update_pfr_entry function; or remote administrators to execute arbitrary SQL commands via the (34) poolname variable in the dpm_get_pool_entry, (35) dpm_insert_fs_entry, (36) dpm_insert_pool_entry, (37) dpm_insert_spcmd_entry, (38) dpm_list_fs_entry, or (39) dpm_update_spcmd_entry function.			
dotclear -- dotclear	Dotclear before 2.6.2 allows remote attackers to execute arbitrary PHP code via a serialized object in the dc_passwd cookie to a password-protected page, which is not properly handled by (1) inc/public/lib.urlhandlers.php or (2) plugins/pages/_public.php.	2014-05-16	7.5	CVE-2014-1613
drupalauth_project -- drupalauth	lib/Auth/Source/External.php in the drupalauth module before 1.2.2 for simpleSAMLphp allows remote attackers to authenticate as an arbitrary user via the user name (uid) in a cookie.	2014-05-13	7.5	CVE-2013-4552
emc -- rsa_netwitness	EMC RSA NetWitness before 9.8.5.19 and RSA Security Analytics before 10.2.4 and 10.3.x	2014-05-16	7.6	CVE-2014-0643

	before 10.3.2, when Kerberos PAM is enabled, do not require a password, which allows remote attackers to bypass authentication by leveraging knowledge of a valid account name.			
f5 -- big-ip_access_policy_manager	The iControl API in F5 BIG-IP LTM, APM, ASM, GTM, Link Controller, and PSM 10.0.0 through 10.2.4 and 11.0.0 through 11.5.1, BIG-IP AAM 11.4.0 through 11.5.1, BIG-IP AFM and PEM 11.3.0 through 11.5.1, BIG-IP Analytics 11.0.0 through 11.5.1, BIG-IP Edge Gateway, WebAccelerator, WOM 10.1.0 through 10.2.4 and 11.0.0 through 11.3.0, Enterprise Manager 2.1.0 through 2.3.0 and 3.0.0 through 3.1.1, and BIG-IQ Cloud, Device, and Security 4.0.0 through 4.3.0 allows remote administrators to execute arbitrary commands via shell metacharacters in the hostname element in a SOAP request.	2014-05-12	7.1	CVE-2014-2928
foscam -- ip_camera_firmware	Foscam IP camera 11.37.2.49 and other versions, when using the Foscam DynDNS option, generates credentials based on predictable camera subdomain names, which allows remote attackers to spoof or hijack arbitrary cameras and conduct other attacks by modifying arbitrary camera records in the Foscam DNS server.	2014-05-13	10.0	CVE-2014-1849
glpi-project -- glpi	Multiple SQL injection vulnerabilities in GLPI before 0.83.9 allow remote attackers to execute arbitrary SQL commands via the (1) users_id_assign parameter to ajax/ticketassigninformation.php, (2) filename parameter to front/document.form.php, or (3) table parameter to ajax/comments.php.	2014-05-14	7.5	CVE-2013-2226
google -- chrome	Multiple use-after-free vulnerabilities in net/websockets/websocket_job.cc in the WebSockets implementation in Google Chrome before 34.0.1847.137 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to WebSocketJob deletion.	2014-05-14	7.5	CVE-2014-1740

google -- chrome	Multiple integer overflows in the replace-data functionality in the CharacterData interface implementation in core/dom/CharacterData.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to ranges.	2014-05-14	7.5	CVE-2014-1741
google -- chrome	Use-after-free vulnerability in the FrameSelection::updateAppearance function in core/editing/FrameSelection.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper RenderObject handling.	2014-05-14	7.5	CVE-2014-1742
google -- android_debug_bridge	Integer signedness error in system/core/adb/adb_client.c in Android Debug Bridge (ADB) for Android 4.4 in the Android SDK Platform Tools 18.0.1 allows ADB servers to execute arbitrary code via a negative length value, which bypasses a signed comparison and triggers a stack-based buffer overflow.	2014-05-13	7.5	CVE-2014-1909
ibm -- websphere_portal	Directory traversal vulnerability in IBM Eclipse Help System (IEHS) 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 CF27, and 8.0 before 8.0.0.1 CF06 allows remote attackers to read arbitrary files via a crafted URL.	2014-05-16	7.1	CVE-2014-0918
ibm -- websphere_application_server	IBM WebSphere Application Server (WAS) 6.1.0.0 through 6.1.0.47 and 6.0.2.0 through 6.0.2.43 allows remote attackers to cause a denial of service via crafted TLS traffic, as demonstrated by traffic from a CVE-2014-0160 vulnerability-assessment tool.	2014-05-16	7.1	CVE-2014-0964
karlen_walter -- si_bibtex	Multiple SQL injection vulnerabilities in the BibTex Publications (si_bibtex) extension 0.2.3 for TYPO3 allow remote attackers to execute arbitrary SQL commands via vectors related to	2014-05-16	7.5	CVE-2014-3759

	the (1) search or (2) list functionality.			
linux -- linux_kernel	The raw_cmd_copyin function in drivers/block/floppy.c in the Linux kernel through 3.14.3 does not properly handle error conditions during processing of an FDRAWCMD ioctl call, which allows local users to trigger kfree operations and gain privileges by leveraging write access to a /dev/fd device.	2014-05-11	7.2	CVE-2014-1737
marc_lehmann -- rxvt-unicode	rxvt-unicode before 9.20 does not properly handle OSC escape sequences, which allows user-assisted remote attackers to manipulate arbitrary X window properties and execute arbitrary commands.	2014-05-13	7.6	CVE-2014-3121
mark_evans -- fog-dragonfly	lib/dragonfly/imagemagickutils.rb in the fog-dragonfly gem 0.8.2 for Ruby allows remote attackers to execute arbitrary commands via unspecified vectors.	2014-05-12	7.5	CVE-2013-5671
mediawiki -- mediawiki	Buffer overflow in php-luasandbox in the Scribuntu extension for MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 has unspecified impact and remote vectors.	2014-05-12	7.5	CVE-2013-4571
mediawiki -- mediawiki	MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 does not properly sanitize SVG files, which allows remote attackers to have unspecified impact via invalid XML.	2014-05-12	7.5	CVE-2013-6453
microsoft -- office_web_apps_server	Microsoft Windows SharePoint Services 3.0 SP3; SharePoint Server 2007 SP3, 2010 SP1 and SP2, and 2013 Gold and SP1; SharePoint Foundation 2010 SP1 and SP2 and 2013 Gold and SP1; Project Server 2010 SP1 and SP2 and 2013 Gold and SP1; Web Applications 2010 SP1 and SP2; Office Web Apps Server 2013 Gold and SP1; SharePoint Server 2013 Client Components SDK; and SharePoint Designer 2007 SP3, 2010 SP1 and SP2, and 2013 Gold and SP1 allow remote authenticated users to execute arbitrary code via crafted page content, aka "SharePoint Page	2014-05-14	9.0	CVE-2014-0251

	Content Vulnerability."			
microsoft -- internet_explorer	Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1815.	2014-05-14	9.3	CVE-2014-0310
microsoft -- office	Untrusted search path vulnerability in Microsoft Office 2007 SP3, 2010 SP1 and SP2, and 2013 Gold, SP1, RT, and RT SP1, when the Simplified Chinese Proofing Tool is enabled, allows local users to gain privileges via a Trojan horse DLL in the current working directory, as demonstrated by a directory that contains a .docx file, aka "Microsoft Office Chinese Grammar Checking Vulnerability."	2014-05-14	7.2	CVE-2014-1756
microsoft -- .net_framework	The .NET Remoting implementation in Microsoft .NET Framework 1.1 SP1, 2.0 SP2, 3.5, 3.5.1, 4, 4.5, and 4.5.1 does not properly restrict memory access, which allows remote attackers to execute arbitrary code via vectors involving malformed objects, aka "TypeFilterLevel Vulnerability."	2014-05-14	10.0	CVE-2014-1806
microsoft -- windows_7	The ShellExecute API in Windows Shell in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 does not properly implement file associations, which allows local users to gain privileges via a crafted application, as exploited in the wild in May 2014, aka "Windows Shell File Association Vulnerability."	2014-05-14	7.2	CVE-2014-1807
microsoft -- web_applications	Microsoft Web Applications 2010 SP1 and SP2 allows remote authenticated users to execute arbitrary code via crafted page content, aka "Web Applications Page Content Vulnerability."	2014-05-14	9.3	CVE-2014-1813
microsoft --	Microsoft Internet Explorer 6 through 11 allows	2014-05-14	9.3	CVE-2014-1815

internet_explorer	remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, as exploited in the wild in May 2014, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-0310.			
oracle -- openjdk	Unspecified vulnerability in OpenJDK 6 before 6b31 on Debian GNU/Linux and Ubuntu 12.04 LTS and 10.04 LTS has unknown impact and attack vectors, a different vulnerability than CVE-2014-2405.	2014-05-13	10.0	CVE-2014-0462
oracle -- openjdk	Unspecified vulnerability in OpenJDK 6 before 6b31 on Debian GNU/Linux and Ubuntu 12.04 LTS and 10.04 LTS has unknown impact and attack vectors, a different vulnerability than CVE-2014-0462.	2014-05-13	10.0	CVE-2014-2405
pcman's_ftp_server_project -- pcman's_ftp_server	Buffer overflow in PCMan's FTP Server 2.0.7 allows remote attackers to execute arbitrary code via a long string in a USER command.	2014-05-15	10.0	CVE-2013-4730
phpmanufaktur -- kitform	SQL injection vulnerability in sorter.php in the phpManufaktur kitForm extension 0.43 and earlier for the KeepInTouch (KIT) module allows remote attackers to execute arbitrary SQL commands via the sorter_value parameter.	2014-05-15	7.5	CVE-2014-3757
symantec -- workspace_streaming	The server in Symantec Workspace Streaming (SWS) before 7.5.0.749 allows remote attackers to access files and functionality by sending a crafted XMLRPC request over HTTPS.	2014-05-16	7.9	CVE-2014-1649
x -- libxfont	Multiple buffer overflows in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs protocol reply to the (1) _fs_recv_conn_setup, (2) fs_read_open_font, (3) fs_read_query_info, (4) fs_read_extent_info, (5) fs_read_glyphs, (6) fs_read_list, or (7) fs_read_list_info function.	2014-05-15	7.5	CVE-2014-0210
x -- libxfont	Multiple integer overflows in the (1) fs_get_reply, (2) fs_alloc_glyphs, and (3)	2014-05-15	7.5	CVE-2014-0211

	fs_read_extent_info functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs reply, which triggers a buffer overflow.			

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- acrobat	Adobe Reader and Acrobat 10.x before 10.1.10 and 11.x before 11.0.07 on Windows and OS X do not properly implement JavaScript APIs, which allows remote attackers to obtain sensitive information via a crafted PDF document.	2014-05-14	4.3	CVE-2014-0521
atlassian -- confluence	Cross-site request forgery (CSRF) vulnerability in logout.action in Atlassian Confluence 3.4.6 allows remote attackers to hijack the authentication of administrators for requests that logout the user.	2014-05-13	6.8	CVE-2012-6342
bilyoner -- bilyoner	The Bilyoner application before 2.3.1 for Android and before 4.6.2 for iOS does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.	2014-05-16	5.8	CVE-2014-3750
bmc -- patrol_agent	Untrusted search path vulnerability in BMC Patrol for AIX 3.9.00 allows local users to gain privileges via a crafted library, related to an incorrect RPATH setting.	2014-05-13	6.9	CVE-2014-2591
bscw -- bscw	OrbiTeam BSCW before 5.0.8 allows remote	2014-05-12	5.0	CVE-2014-2301

	attackers to obtain sensitive metadata via the inf operations (op=inf) to an object in pub/bscw.cgi/.			
cagintranetworks -- getsimple_cms	Multiple cross-site scripting (XSS) vulnerabilities in GetSimple CMS 3.3.1 allow remote attackers to inject arbitrary web script or HTML via the (1) param parameter to admin/load.php or (2) user, (3) email, or (4) name parameter in a Save Settings action to admin/settings.php.	2014-05-14	4.3	CVE-2014-1603
canonical -- software-properties	ppa.py in Software Properties before 0.81.13.3 does not validate the server certificate when downloading PPA GPG key fingerprints, which allows man-in-the-middle (MITM) attackers to spoof GPG keys for a package repository.	2014-05-13	4.3	CVE-2011-4407
cisco -- ios	The Locator/ID Separation Protocol (LISP) implementation in Cisco IOS 15.3(3)S and earlier and IOS XE does not properly validate parameters in ITR control messages, which allows remote attackers to cause a denial of service (CEF outage and packet drops) via malformed messages, aka Bug ID CSCun73782.	2014-05-16	4.3	CVE-2014-3262
cisco -- ios	The ScanSafe module in Cisco IOS 15.3(3)M allows remote attackers to cause a denial of service (device reload) via HTTPS packets that require tower processing, aka Bug ID CSCum97038.	2014-05-16	5.4	CVE-2014-3263
cloudbees -- jenkins	Multiple cross-site request forgery (CSRF) vulnerabilities in CloudBees Jenkins before 1.514, LTS before 1.509.1, and Enterprise 1.466.x before 1.466.14.1 and 1.480.x before 1.480.4.1 allow remote attackers to hijack the authentication of administrators for requests that (1) execute arbitrary code or (2) initiate deployment of binaries to a Maven repository via unspecified vectors.	2014-05-14	6.8	CVE-2013-2034
cobblerd -- cobbler	Absolute path traversal vulnerability in the web interface in Cobbler 2.4.x through 2.6.x allows remote authenticated users to read arbitrary files via the Kickstart field in a profile.	2014-05-13	4.0	CVE-2014-3225
d-link -- dap_1150	Multiple cross-site request forgery (CSRF) vulnerabilities in D-Link DAP 1150 with firmware	2014-05-16	6.8	CVE-2014-3760

	1.2.94 allow remote attackers to hijack the authentication of administrators for requests that (1) enable or (2) disable the DMZ in the Firewall/DMZ section via a request to index.cgi or (3) add, (4) modify, or (5) delete URL-filter settings in the Control/URL-filter section via a request to index.cgi, as demonstrated by adding a rule that blocks access to google.com.			
d-link -- dap_1150	Cross-site scripting (XSS) vulnerability in D-Link DAP 1150 with firmware 1.2.94 allows remote attackers to inject arbitrary web script or HTML via the res_buf parameter to index.cgi in the Control/URL-filter section.	2014-05-16	4.3	CVE-2014-3761
djangoproject -- django	Django 1.4 before 1.4.13, 1.5 before 1.5.8, 1.6 before 1.6.5, and 1.7 before 1.7b4 does not properly include the (1) Vary: Cookie or (2) Cache-Control header in responses, which allows remote attackers to obtain sensitive information or poison the cache via a request from certain browsers.	2014-05-16	6.4	CVE-2014-1418
djangoproject -- django	The django.util.http.is_safe_url function in Django 1.4 before 1.4.13, 1.5 before 1.5.8, 1.6 before 1.6.5, and 1.7 before 1.7b4 does not properly validate URLs, which allows remote attackers to conduct open redirect attacks via a malformed URL, as demonstrated by "http:\\\djangoproject.com."	2014-05-16	4.3	CVE-2014-3730
dovecot -- dovecot	Dovecot 1.1 before 2.2.13 and dovecot-ee before 2.1.7.7 and 2.2.x before 2.2.12.12 does not properly close old connections, which allows remote attackers to cause a denial of service (resource consumption) via an incomplete SSL/TLS handshake for an IMAP/POP3 connection.	2014-05-14	5.0	CVE-2014-3430
galleryproject -- gallery	Multiple cross-site scripting (XSS) vulnerabilities in Gallery 3 before 3.0.7 allow remote attackers to inject arbitrary web script or HTML via the (1) movie title to modules/gallery/controllers/movies.php or (2) key variable to modules/gallery/views/error_admin.html.php.	2014-05-14	4.3	CVE-2013-2087
gitlab -- gitlab	The SSH key upload feature (lib/gitlab_keys.rb) in	2014-05-13	6.5	CVE-2013-4490

	gitlab-shell before 1.7.3, as used in GitLab 5.0 before 5.4.1 and 6.x before 6.2.3, allows remote authenticated users to execute arbitrary commands via shell metacharacters in the public key.			
gitlab -- gitlab	The repository import feature in gitlab-shell before 1.7.4, as used in GitLab, allows remote authenticated users to execute arbitrary commands via the import URL.	2014-05-13	6.5	CVE-2013-4546
gitlab -- gitlab	GitLab before 5.4.2, Community Edition before 6.2.4, and Enterprise Edition before 6.2.1, when using a MySQL backend, allows remote attackers to impersonate arbitrary users and bypass authentications via unspecified API calls.	2014-05-12	6.8	CVE-2013-4580
gitlab -- gitlab	GitLab 5.0 before 5.4.2, Community Edition before 6.2.4, Enterprise Edition before 6.2.1 and gitlab-shell before 1.7.8 allows remote attackers to execute arbitrary code via a crafted change using SSH.	2014-05-12	6.8	CVE-2013-4581
gitlab -- gitlab	Cross-site scripting (XSS) vulnerability in GitLab Enterprise Edition (EE) 6.6.0 before 6.6.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-13	4.3	CVE-2014-3456
google -- android	Android OS before 2.2 does not display the correct SSL certificate in certain cases, which might allow remote attackers to spoof trusted web sites via a web page containing references to external sources in which (1) the certificate of the last loaded resource is checked, instead of for the main page, or (2) later certificates are not checked when the HTTPS connection is reused.	2014-05-13	4.3	CVE-2010-4832
hp -- network_node_manager_i	Cross-site scripting (XSS) vulnerability in HP Network Node Manager i (NNMi) 9.0, 9.10, and 9.20 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2014-05-09	4.3	CVE-2013-6220
ibm -- websphere_portal	Cross-site scripting (XSS) vulnerability in IBM Eclipse Help System (IEHS) 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 CF27, and 8.0 before 8.0.0.1 CF06	2014-05-16	4.3	CVE-2014-0917

	allows remote attackers to inject arbitrary web script or HTML via a crafted URL.			
ibm -- infosphere_information_server_metadata_workbench	Cross-site request forgery (CSRF) vulnerability in IBM InfoSphere Information Server Metadata Workbench 8.1 through 9.1 allows remote attackers to hijack the authentication of arbitrary users.	2014-05-16	6.8	CVE-2014-0933
icedtea_project -- icedtea-web	The Java Network Launching Protocol (JNLP) implementation in IcedTea6 1.9.x before 1.9.9 and before 1.8.9, and IcedTea-Web 1.1.x before 1.1.1 and before 1.0.4, allows remote attackers to obtain the username and full path of the home and cache directories by accessing properties of the ClassLoader.	2014-05-13	5.0	CVE-2011-2513
icedtea_project -- icedtea-web	The Java Network Launching Protocol (JNLP) implementation in IcedTea6 1.9.x before 1.9.9 and before 1.8.9, and IcedTea-Web 1.1.x before 1.1.1 and before 1.0.4, allows remote attackers to trick victims into granting access to local files by modifying the content of the Java Web Start Security Warning dialog box to represent a different filename than the file for which access will be granted.	2014-05-13	6.8	CVE-2011-2514
intersectalliance -- system_intrusion_analysis_and_reporting_environment	Cross-site scripting (XSS) vulnerability in the events page in the System iNtrusion Analysis and Reporting Environment (SNARE) for Linux agent before 1.7.0 allows remote attackers to inject arbitrary web script or HTML via a logged shell command.	2014-05-14	4.3	CVE-2011-5249
jetaudio -- jetaudio	JetMPAd.ax in JetAudio 8.1.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted .ogg file.	2014-05-14	4.3	CVE-2014-3443
karlen_walter -- si_bibtex	Cross-site scripting (XSS) vulnerability in the BibTex Publications (si_bibtex) extension 0.2.3 for TYPO3 allows remote attackers to inject arbitrary web script or HTML via vectors related to the import functionality.	2014-05-16	4.3	CVE-2014-3758
linux -- linux_kernel	The raw_cmd_copyout function in drivers/block/floppy.c in the Linux kernel through	2014-05-11	4.9	CVE-2014-1738

	3.14.3 does not properly restrict access to certain pointers during processing of an FDRAWCMD ioctl call, which allows local users to obtain sensitive information from kernel heap memory by leveraging write access to a /dev/fd device.			
linux -- linux_kernel	The try_to_unmap_cluster function in mm/rmap.c in the Linux kernel before 3.14.3 does not properly consider which pages must be locked, which allows local users to cause a denial of service (system crash) by triggering a memory-usage pattern that requires removal of page-table mappings.	2014-05-11	4.9	CVE-2014-3122
linux -- linux_kernel	The (1) BPF_S_ANC_NLATTR and (2) BPF_S_ANC_NLATTR_NEST extension implementations in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 do not check whether a certain length value is sufficiently large, which allows local users to cause a denial of service (integer underflow and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr and __skb_get_nlattr_nest functions before the vulnerability was announced.	2014-05-11	4.9	CVE-2014-3144
linux -- linux_kernel	The BPF_S_ANC_NLATTR_NEST extension implementation in the sk_run_filter function in net/core/filter.c in the Linux kernel through 3.14.3 uses the reverse order in a certain subtraction, which allows local users to cause a denial of service (over-read and system crash) via crafted BPF instructions. NOTE: the affected code was moved to the __skb_get_nlattr_nest function before the vulnerability was announced.	2014-05-11	4.9	CVE-2014-3145
lxml -- lxml	Incomplete blacklist vulnerability in the lxml.html.clean module in lxml before 3.3.5 allows remote attackers to conduct cross-site scripting (XSS) attacks via control characters in the link scheme to the clean_html function.	2014-05-14	4.3	CVE-2014-3146
madeofcode -- omniauth-facebook	The omniauth-facebook gem 1.4.1 before 1.5.0 does not properly store the session parameter,	2014-05-13	6.8	CVE-2013-4562

	which allows remote attackers to conduct cross-site request forgery (CSRF) attacks via the state parameter.			
makina-corpus -- soappy	SOAPpy 0.12.5 allows remote attackers to read arbitrary files via a SOAP request containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.	2014-05-12	5.0	CVE-2014-3242
makina-corpus -- soappy	SOAPpy 0.12.5 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 SOAP request containing a large number of nested entity references.	2014-05-12	5.0	CVE-2014-3243
mantisbt -- mantisbt	Cross-site scripting (XSS) vulnerability in the filter_draw_selection_area2 function in core/filter_api.php in MantisBT 1.2.12 before 1.2.13 allows remote attackers to inject arbitrary web script or HTML via the match_type parameter to bugs/search.php.	2014-05-15	4.3	CVE-2013-0197
mediawiki -- mediawiki	The zend_inline_hash_func function in php-luasandbox in the Scribuntu extension for MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via vectors related to converting Lua data structures to PHP, as demonstrated by passing { [{}] = 1 } to a module function.	2014-05-12	5.0	CVE-2013-4570
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in the TimeMediaHandler extension for MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to inject arbitrary web script or HTML via vectors related to videos.	2014-05-12	4.3	CVE-2013-4574
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to inject arbitrary web script or HTML via crafted XSL in an SVG file.	2014-05-12	4.3	CVE-2013-6452
mediawiki --	Cross-site scripting (XSS) vulnerability in MediaWiki	2014-05-12	4.3	CVE-2013-6454

mediawiki	before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to inject arbitrary web script or HTML via a -o-link attribute.			
mediawiki -- mediawiki	MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to obtain information about deleted page via the (1) log API, (2) enhanced RecentChanges, and (3) user watchlists.	2014-05-12	5.0	CVE-2013-6472
mediawiki -- mediawiki	Cross-site request forgery (CSRF) vulnerability in Special:CreateCategory in the SemanticForms extension for MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allows remote attackers to hijack the authentication of users for requests that create categories via unspecified vectors.	2014-05-12	6.8	CVE-2014-3454
mediawiki -- mediawiki	Multiple cross-site request forgery (CSRF) vulnerabilities in the (1) CreateProperty, (2) CreateTemplate, (3) CreateForm, and (4) CreateClass special pages in the SemanticForms extension for MediaWiki before 1.19.10, 1.2x before 1.21.4, and 1.22.x before 1.22.1 allow remote attackers to hijack the authentication of users for requests that have unspecified impact and vectors.	2014-05-12	6.8	CVE-2014-3455
microsoft -- windows_server_2008	Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold and R2 allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka "iSCSI Target Remote Denial of Service Vulnerability."	2014-05-14	5.0	CVE-2014-0255
microsoft -- windows_server_2008	Microsoft Windows Server 2008 SP2 and R2 SP1 and Server 2012 Gold allow remote attackers to cause a denial of service (iSCSI service outage) by sending many crafted packets, aka "iSCSI Target Remote Denial of Service Vulnerability."	2014-05-14	5.0	CVE-2014-0256
microsoft -- office_web_apps_server	Cross-site scripting (XSS) vulnerability in Microsoft SharePoint Server 2013 Gold and SP1, SharePoint Foundation 2013 Gold and SP1, Office Web Apps Server 2013 Gold and SP1, and SharePoint Server 2013 Client Components SDK allows remote	2014-05-14	4.3	CVE-2014-1754

	attackers to inject arbitrary web script or HTML via a crafted request, aka "SharePoint XSS Vulnerability."			
microsoft -- office	Microsoft Office 2013 Gold, SP1, RT, and RT SP1 allows remote attackers to obtain sensitive token information via a web site that sends a crafted response during opening of an Office document, aka "Token Reuse Vulnerability."	2014-05-14	4.3	CVE-2014-1808
microsoft -- office	The MSCOMCTL library in Microsoft Office 2007 SP3, 2010 SP1 and SP2, and 2013 Gold, SP1, RT, and RT SP1 makes it easier for remote attackers to bypass the ASLR protection mechanism via a crafted web site, as exploited in the wild in May 2014, aka "MSCOMCTL ASLR Vulnerability."	2014-05-14	6.8	CVE-2014-1809
microsoft -- windows_7	The Group Policy implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly handle distribution of passwords, which allows remote authenticated users to obtain sensitive credential information and consequently gain privileges by leveraging access to the SYSVOL share, as exploited in the wild in May 2014, aka "Group Policy Preferences Password Elevation of Privilege Vulnerability."	2014-05-14	6.8	CVE-2014-1812
microweber -- microweber	Directory traversal vulnerability in userfiles/modules/admin/backup/delete.php in Microweber before 0.830 allows remote attackers to delete arbitrary files via a .. (dot dot) in the file parameter.	2014-05-12	6.4	CVE-2013-5984
nathan_haug -- filefield_sources	The FileField Sources module 6.x-1.x before 6.x-1.9 and 7.x-1.x before 7.x-1.9 for Drupal does not properly check file permissions, which allows remote authenticated users to read arbitrary files by attaching a file.	2014-05-13	4.0	CVE-2013-4502
netweblogic -- events_manager	Multiple cross-site scripting (XSS) vulnerabilities in the Events Manager plugin before 5.3.5 and Events Manager Pro plugin before 2.2.9 for WordPress allow remote attackers to inject arbitrary web script	2014-05-13	4.3	CVE-2013-1407

	or HTML via the (1) scope parameter to index.php; (2) user_name, (3) dbem_phone, (4) user_email, or (5) booking_comment parameter to and event with registration enabled; or the (6) _wpnonce parameter to wp-admin/edit.php.			
o-dyn -- collabtive	SQL injection vulnerability in Collabtive 1.2 allows remote authenticated users to execute arbitrary SQL commands via the folder parameter in a fileview_list action to manageajax.php.	2014-05-13	6.5	CVE-2014-3246
o-dyn -- collabtive	Cross-site scripting (XSS) vulnerability in Collabtive 1.2 allows remote authenticated users to inject arbitrary web script or HTML via the desc parameter in an Add project (addpro) action to admin.php.	2014-05-15	4.3	CVE-2014-3247
open_assessment_technologies_ -- tao	Cross-site request forgery (CSRF) vulnerability in Open Assessment Technologies TAO 2.5.6 allows remote attackers to hijack the authentication of administrators for requests that create administrative accounts via a request to Users/add.	2014-05-13	6.8	CVE-2014-2989
openstack -- horizon	The Identity v3 API in OpenStack Dashboard (Horizon) before 2013.2 does not require the current password when changing passwords for user accounts, which makes it easier for remote attackers to change a user password by leveraging the authentication token for that user.	2014-05-14	5.0	CVE-2013-4471
openvpn -- openvpn_access_server	Cross-site request forgery (CSRF) vulnerability in the Admin web interface in OpenVPN Access Server before 1.8.5 allows remote attackers to hijack the authentication of administrators for requests that create administrative users.	2014-05-13	6.8	CVE-2013-2692
openx -- openx	Multiple directory traversal vulnerabilities in OpenX before 2.8.10 revision 82710 allow remote administrators to read arbitrary files via a .. (dot dot) in the group parameter to (1) plugin-preferences.php or (2) plugin-settings.php in www/admin, a different vulnerability than CVE-2013-7376. NOTE: this can be leveraged using CSRF to allow remote unauthenticated attackers to read arbitrary files.	2014-05-14	4.3	CVE-2013-3514

openx -- openx	Multiple cross-site request forgery (CSRF) vulnerabilities in OpenX 2.8.10, possibly before revision 82710, allow remote attackers to hijack the authentication of administrators, as demonstrated by requests that conduct directory traversal attacks via the group parameter to (1) plugin-preferences.php or (2) plugin-settings.php in www/admin, a different vulnerability than CVE-2013-3514.	2014-05-14	6.8	CVE-2013-7376
phpcms -- guesbook_module	Multiple cross-site scripting (XSS) vulnerabilities in the Guestbook module for PHPCMS allow remote attackers to inject arbitrary web script or HTML via the (1) list or (2) introduce parameter to index.php.	2014-05-14	4.3	CVE-2013-5939
phppgadmin_project -- phppgadmin	Multiple cross-site scripting (XSS) vulnerabilities in functions.php in phpPgAdmin before 5.0.4 allow remote attackers to inject arbitrary web script or HTML via the (1) name or (2) type of a function.	2014-05-13	4.3	CVE-2012-1600
quiz_module_project -- quiz	The Quiz module 6.x-4.x before 6.x-4.5 for Drupal allows remote authenticated users with the "view any quiz results" or "view results for own quiz" permission to delete arbitrary results via the delete option.	2014-05-13	4.9	CVE-2013-4500
quiz_module_project -- quiz	The default views in the Quiz module 6.x-4.x before 6.x-4.5 for Drupal allows remote attackers to obtain sensitive quiz results via unspecified vectors.	2014-05-13	5.0	CVE-2013-4501
redhat -- cloudforms_3.0_management_engine	The CatalogController in Red Hat CloudForms Management Engine (CFME) before 5.2.3.2 allows remote authenticated users to delete arbitrary catalogs via vectors involving guessing the catalog ID.	2014-05-14	4.0	CVE-2014-0078
redhat -- cloudforms_3.0_management_engine	SQL injection vulnerability in the saved_report_delete action in the ReportController in Red Hat CloudForms Management Engine (CFME) before 5.2.3.2 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors, related to MiqReportResult.exists.	2014-05-14	6.5	CVE-2014-0137
simplerisk -- simplerisk	Cross-site request forgery (CSRF) vulnerability in management/prioritize_planning.php in	2014-05-12	6.8	CVE-2013-5748

	SimpleRisk before 20130916-001 allows remote attackers to hijack the authentication of users for requests that add projects via an add_project action.			
simplerisk -- simplerisk	Cross-site scripting (XSS) vulnerability in management/prioritize_planning.php in SimpleRisk before 20130916-001 allows remote attackers to inject arbitrary web script or HTML via the new_project parameter.	2014-05-12	4.3	CVE-2013-5749
smart-flv_plugin_project -- smart-flv	Multiple cross-site scripting (XSS) vulnerabilities in jwplayer.swf in the smart-flv plugin for WordPress allow remote attackers to inject arbitrary web script or HTML via the (1) link or (2) playerready parameter.	2014-05-14	4.3	CVE-2013-1765
tipsandtricks-hq -- wordpress_simple_paypal_shopping_cart	Cross-site request forgery (CSRF) vulnerability in the WordPress Simple Paypal Shopping Cart plugin before 3.6 for WordPress allows remote attackers to hijack the authentication of administrators for requests that change plugin settings.	2014-05-13	6.8	CVE-2013-2705
ucdok -- tomato	The admin API in the tomato module before 0.0.6 for Node.js does not properly check the access key when it is set to a string, which allows remote attackers to bypass authentication via a string in the access-key header that partially matches config.master.api.access_key.	2014-05-16	6.8	CVE-2013-7379
vicidial -- vicidial	VICIDIAL dialer (aka Asterisk GUI client) 2.8-403a, 2.7, 2.7RC1, and earlier allows remote authenticated users to execute arbitrary commands via shell metacharacters in the extension parameter in an OriginateVDRelogin action to manager_send.php.	2014-05-14	6.5	CVE-2013-4468
videolan -- vlc_media_player	codec\libpng_plugin.dll in VideoLAN VLC Media Player 2.1.3 allows remote attackers to cause a denial of service (crash) via a crafted .png file, as demonstrated by a png in a .wave file.	2014-05-14	4.3	CVE-2014-3441
webmaster-source -- wp125	Cross-site request forgery (CSRF) vulnerability in the Add/Edit page (adminmenus.php) in the WP125 plugin before 1.5.0 for WordPress allows remote attackers to hijack the authentication of	2014-05-14	6.8	CVE-2013-2700

	administrators for requests that add or edit an ad via unspecified vectors.			
x -- libxfont	Multiple integer overflows in the (1) FontFileAddEntry and (2) lexAlias functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 might allow local users to gain privileges by adding a directory with a large fonts.dir or fonts.alias file to the font path, which triggers a heap-based buffer overflow, related to metadata.	2014-05-15	4.6	CVE-2014-0209
xiaowen_huang -- yingzhi_python_programming_language	Directory traversal vulnerability in the FTP server in YingZhi Python Programming Language for iOS 1.9 allows remote attackers to read and possibly write arbitrary files via a .. (dot dot) in the default URI.	2014-05-14	6.4	CVE-2013-5655

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
feed_element_mapper_project -- feed_element_mapper	Cross-site scripting (XSS) vulnerability in the Feed Element Mapper module for Drupal allows remote authenticated users with the "administer taxonomy" permission to inject arbitrary web script or HTML via vectors related to options.	2014-05-13	2.1	CVE-2013-4503
gnu -- grub	A certain Debian patch for GNU GRUB uses world-readable permissions for grub.cfg, which allows local users to obtain password hashes, as demonstrated by reading the password_pbkdf2 directive in the file.	2014-05-12	2.1	CVE-2013-4577
hp -- 8/20q_fibre_chann	Unspecified vulnerability on HP 8/20q switches, SN6000 switches, and 8Gb Simple SAN Connection	2014-05-09	1.7	CVE-2014-2603

el_switch_16_port	Kit with firmware before 8.0.14.08.00 allows remote authenticated users to obtain sensitive information via unknown vectors.			
katello -- katello_installer	Katello Installer before 0.0.18 uses world-readable permissions for /etc/pki/tls/private/katello-node.key when deploying a child Pulp node, which allows local users to obtain the private key by reading the file.	2014-05-14	2.1	CVE-2013-4455
mantisbt -- mantisbt	Multiple cross-site scripting (XSS) vulnerabilities in core/summary_api.php in MantisBT 1.2.12 allow remote authenticated users with manager or administrator permissions to inject arbitrary web script or HTML via a (1) category name in the summary_print_by_category function or (2) project name in the summary_print_by_project function.	2014-05-15	2.1	CVE-2013-1810
monster_menus_module_project -- monster_menus	The Monster Menus module 7.x-1.x before 7.x-1.15 allows remote attackers to read arbitrary node comments via a crafted URL.	2014-05-13	2.6	CVE-2013-4504

- 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).