Vulnerability Summary for the Week of September 16, 2013 - Bulletin (SB13-266)

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
Back to top				
apple -- itunes	The iTunes ActiveX control in Apple iTunes before 11.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.	2013-09-19	9.3	CVE-2013-1035
apple -- iphone_os	The IOSerialFamily driver in Apple iOS before 7 allows attackers to execute arbitrary code or cause a denial of service (out-of-bounds array access) via a crafted application.	2013-09-19	9.3	CVE-2013-5139
apple -- iphone_os	The kernel in Apple iOS before 7 allows remote attackers to cause a denial of service (assertion failure and device restart) via an invalid packet fragment.	2013-09-19	7.8	CVE-2013-5140
apple -- iphone_os	The kernel in Apple iOS before 7 uses an incorrect data size for a certain integer variable, which allows attackers to cause a denial of service (infinite loop and device hang) via a crafted application, related to an "integer truncation vulnerability."	2013-09-19	7.1	CVE-2013-5141
apple -- iphone_os	The Sandbox subsystem in Apple iOS before 7 allows attackers to cause a denial of service (infinite loop) via an application that writes crafted values to /dev/random.	2013-09-19	7.1	CVE-2013-5155
dahuasecurity -- dvr0404hd-a	Dahua DVR appliances have a hardcoded password for (1) the root account and (2) an unspecified "backdoor" account, which makes it easier for remote attackers to obtain administrative access via authorization requests involving (a) ActiveX, (b) a standalone client, or (c) unknown other vectors.	2013-09-17	10.0	CVE-2013-3612
dahuasecurity -- dvr0404hd-a	Dahua DVR appliances do not properly restrict UPnP requests, which makes it easier for remote attackers to obtain access via vectors involving a replay attack against the TELNET port.	2013-09-17	7.8	CVE-2013-3613
dahuasecurity -- dvr0404hd-a	Dahua DVR appliances have a small value for the maximum password length, which makes it easier for remote attackers to obtain access via a brute-force attack.	2013-09-17	9.3	CVE-2013-3614

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
dahuasecurity -- dvr0404hd-a	Dahua DVR appliances use a password-hash algorithm with a short hash length, which makes it easier for context-dependent attackers to discover cleartext passwords via a brute-force attack.	2013-09-17	7.8	CVE-2013-3615
dahuasecurity -- dvr0404hd-a	The authorization implementation on Dahua DVR appliances accepts a hash string representing the current date for the role of a master password, which makes it easier for remote attackers to obtain administrative access and change the administrator password via requests involving (1) ActiveX, (2) a standalone client, or (3) unspecified other vectors, a different vulnerability than CVE-2013-3612.	2013-09-17	10.0	CVE-2013-5754
hp -- identity_driven_manager	Multiple SQL injection vulnerabilities in GetEventsServlet in HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, and Identity Driven Manager (IDM) 4.0 allow remote attackers to execute arbitrary SQL commands via the (1) sort or (2) dir parameter.	2013-09-16	7.5	CVE-2013-4809
hp -- application_lifecycle_management	HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, Identity Driven Manager (IDM) 4.0, and Application Lifecycle Management allow remote attackers to execute arbitrary code via a marshalled object to (1) EJBInvokerServlet or (2) JMXInvokerServlet, aka ZDI-CAN-1760.	2013-09-16	10.0	CVE-2013-4810
hp -- identity_driven_manager	UpdateDomainControllerServlet in the SNAC registration server in HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, and Identity Driven Manager (IDM) 4.0 does not properly validate the adCert argument, which allows remote attackers to upload .jsp files and consequently execute arbitrary code via unspecified vectors, aka ZDI-CAN-1743.	2013-09-16	10.0	CVE-2013-4811
hp -- identity_driven_manager	UpdateCertificatesServlet in the SNAC registration server in HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, and Identity Driven Manager (IDM) 4.0 does not properly validate the fileName argument, which allows remote attackers to upload .jsp files and consequently execute arbitrary code via unspecified vectors, aka ZDI-CAN-1743.	2013-09-16	10.0	CVE-2013-4812
hp -- identity_driven_manager	The Agent (aka AgentController) servlet in HP ProCurve Manager (PCM) 3.20 and 4.0, PCM+ 3.20 and 4.0, and Identity Driven Manager (IDM) 4.0 allows remote attackers to execute arbitrary commands via a HEAD request, aka ZDI-	2013-09-16	10.0	CVE-2013-4813

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	CAN-1745.			
ibm -- spss_analytical_decision_management	Unrestricted file upload vulnerability in IBM SPSS Analytical Decision Management 6.1 before IF1, 6.2 before IF1, and 7.0 before FP1 IF6 allows remote authenticated users to execute arbitrary code by uploading and accessing a JSP file.	2013-09-16	9.0	CVE-2013-4049
ibm -- spss_analytical_decision_management	IBM SPSS Analytical Decision Management 6.1 before IF1, 6.2 before IF1, and 7.0 before FP1 IF6 might allow remote attackers to execute arbitrary code by deploying and accessing a service.	2013-09-16	9.3	CVE-2013-5369
microsoft -- internet_explorer	Use-after-free vulnerability in the SetMouseCapture implementation in mshtml.dll in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code via crafted JavaScript strings, as demonstrated by use of an ms-help: URL that triggers loading of hxds.dll.	2013-09-18	9.3	CVE-2013-3893
moodle -- moodle	Moodle through 2.2.11, 2.3.x before 2.3.9, 2.4.x before 2.4.6, and 2.5.x before 2.5.2 does not prevent use of '\0' characters in query strings, which might allow remote attackers to conduct SQL injection attacks against Microsoft SQL Server via a crafted string.	2013-09-16	7.5	CVE-2013-4313
moodle -- moodle	badges/external.php in Moodle 2.5.x before 2.5.2 does not properly handle an object obtained by unserializing a description of an external badge, which allows remote attackers to conduct PHP object injection attacks via unspecified vectors, as demonstrated by overwriting the value of the userid parameter.	2013-09-16	7.5	CVE-2013-5674
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2013-09-18	10.0	CVE-2013-1718
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2013-09-18	10.0	CVE-2013-1719
mozilla -- firefox	The nsHtml5TreeBuilder::resetTheInsertionMode function in the HTML5 Tree	2013-09-18	7.5	CVE-2013-1720

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Builder in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 does not properly maintain the state of the insertion-mode stack for template elements, which allows remote attackers to execute arbitrary code or cause a denial of service (heap-based buffer over-read) by triggering use of this stack in its empty state.			
mozilla -- firefox	Use-after-free vulnerability in the nsAnimationManager::BuildAnimations function in the Animation Manager in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving stylesheet cloning.	2013-09-18	9.3	CVE-2013-1722
mozilla -- firefox	Use-after-free vulnerability in the mozilla::dom::HTMLFormElement::IsDefaultSubmitElement function in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via vectors involving a destroyed SELECT element.	2013-09-18	9.3	CVE-2013-1724
mozilla -- firefox	Untrusted search path vulnerability in the GL tracing functionality in Mozilla Firefox before 24.0 on Android allows attackers to execute arbitrary code via a Trojan horse .so file in a world-writable directory.	2013-09-18	9.3	CVE-2013-1731
mozilla -- firefox	Buffer overflow in the nsFloatManager::GetFlowArea function in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code via crafted use of lists and floats within a multi-column layout.	2013-09-18	9.3	CVE-2013-1732
mozilla -- firefox	Use-after-free vulnerability in the mozilla::layout::ScrollbarActivity function in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code via vectors related to image-document scrolling.	2013-09-18	9.3	CVE-2013-1735
mozilla -- firefox	The nsGfxScrollFrameInner::IsLTR function in Mozilla Firefox before 24.0,	2013-09-18	10.0	CVE-2013-1736

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to improperly establishing parent-child relationships of range-request nodes.			
mozilla -- firefox	Use-after-free vulnerability in the JS_GetGlobalForScopeChain function in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 allows remote attackers to execute arbitrary code by leveraging incorrect garbage collection in situations involving default compartments and frame-chain restoration.	2013-09-18	9.3	CVE-2013-1738
redhat -- openstack	app/controllers/api/v1/hosts_controller.rb in Foreman before 1.2.2 does not properly restrict access to hosts, which allows remote attackers to access arbitrary hosts via an API request.	2013-09-16	7.5	CVE-2013-4182
siemens -- scalance_x-200	The authentication implementation in the web server on Siemens SCALANCE X-200 switches with firmware before 5.0.0 does not use a sufficient source of entropy for generating values of random numbers, which makes it easier for remote attackers to hijack sessions by predicting a value.	2013-09-17	8.3	CVE-2013-5709
Medium Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
Back to top				
apple -- iphone_os	The IPv6 implementation in the kernel in Apple iOS before 7 allows remote attackers to cause a denial of service (CPU consumption) via crafted ICMPv6 packets.	2013-09-19	6.1	CVE-2011-2391
apple -- iphone_os	Data Protection in Apple iOS before 7 allows attackers to bypass intended limits on incorrect passcode entry, and consequently avoid a configured Erase Data setting, by leveraging the presence of an app in the third-party sandbox.	2013-09-19	5.8	CVE-2013-0957
apple -- mac_os_x	Buffer overflow in CoreGraphics in Apple Mac OS X before 10.8.5 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted JBIG2 data in a PDF document.	2013-09-16	6.8	CVE-2013-1025
apple -- mac_os_x	Buffer overflow in ImageIO in Apple Mac OS X before 10.8.5 allows remote	2013-09-16	6.8	CVE-2013-1026

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	attackers to execute arbitrary code or cause a denial of service (application crash) via crafted JPEG2000 data in a PDF document.			
apple -- mac_os_x	Installer in Apple Mac OS X before 10.8.5 provides an option to continue a package's installation after encountering a revoked certificate, which might allow user-assisted remote attackers to execute arbitrary code via a crafted package.	2013-09-16	6.8	CVE-2013-1027
apple -- mac_os_x	The IPSec implementation in Apple Mac OS X before 10.8.5, when Hybrid Auth is used, does not verify X.509 certificates from security gateways, which allows man-in-the-middle attackers to spoof security gateways and obtain sensitive information via a crafted certificate.	2013-09-16	5.8	CVE-2013-1028
apple -- mac_os_x	The kernel in Apple Mac OS X before 10.8.5 allows remote attackers to cause a denial of service (panic) via crafted IGMP packets that leverage incorrect, extraneous code in the IGMP parser.	2013-09-16	4.9	CVE-2013-1029
apple -- quicktime	QuickTime in Apple Mac OS X before 10.8.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted idsc atom in a QuickTime movie file.	2013-09-16	6.8	CVE-2013-1032
apple -- mac_os_x	Screen Lock in Apple Mac OS X before 10.8.5 does not properly track sessions, which allows remote authenticated users to bypass locking by leveraging screen-sharing access.	2013-09-16	5.5	CVE-2013-1033
apple -- os_x_server	Multiple cross-site scripting (XSS) vulnerabilities in Wiki Server in Apple Mac OS X Server before 2.2.2 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2013-09-19	4.3	CVE-2013-1034
apple -- iphone_os	Safari in Apple iOS before 7 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.	2013-09-19	6.8	CVE-2013-1036
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1037
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs	2013-09-19	6.8	CVE-2013-1038

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	listed in APPLE-SA-2013-09-18-2.			
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1039
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1040
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1041
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1042
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1043
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1044
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1045
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute	2013-09-19	6.8	CVE-2013-1046

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.			
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-1047
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-5125
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-5126
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-5127
apple -- iphone_os	WebKit, as used in Apple iOS before 7, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2013-09-18-2.	2013-09-19	6.8	CVE-2013-5128
apple -- iphone_os	Multiple cross-site scripting (XSS) vulnerabilities in WebKit in Apple iOS before 7 allow user-assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.	2013-09-19	4.3	CVE-2013-5129
apple -- iphone_os	Cross-site scripting (XSS) vulnerability in WebKit in Apple iOS before 7 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.	2013-09-19	4.3	CVE-2013-5131
apple -- iphone_os	The kernel in Apple iOS before 7 does not initialize unspecified kernel data structures, which allows local users to obtain sensitive information from kernel	2013-09-19	4.9	CVE-2013-5142

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	stack memory via the (1) msgctl API or (2) segctl API.			
apple -- iphone_os	Passcode Lock in Apple iOS before 7 does not properly manage the lock state, which allows physically proximate attackers to bypass an intended passcode requirement by leveraging a race condition involving phone calls and ejection of a SIM card.	2013-09-19	6.2	CVE-2013-5147
apple -- iphone_os	The Push Notifications subsystem in Apple iOS before 7 provides the push-notification token to an app without user approval, which allows attackers to obtain sensitive information via an app that employs a crafted push-notification registration process.	2013-09-19	4.3	CVE-2013-5149
apple -- iphone_os	Mobile Safari in Apple iOS before 7 does not prevent HTML interpretation of a document served with a text/plain content type, which allows remote attackers to conduct cross-site scripting (XSS) attacks by uploading a file.	2013-09-19	4.3	CVE-2013-5151
apple -- iphone_os	Mobile Safari in Apple iOS before 7 allows remote attackers to spoof the URL bar via a crafted web site.	2013-09-19	4.3	CVE-2013-5152
apple -- iphone_os	The Sandbox subsystem in Apple iOS before 7 determines the sandboxing requirement for a #! application on the basis of the script interpreter instead of the script, which allows attackers to bypass intended access restrictions via a crafted application.	2013-09-19	4.3	CVE-2013-5154
apple -- iphone_os	The Telephony subsystem in Apple iOS before 7 does not require API conformity for access to telephony-daemon interfaces, which allows attackers to bypass intended restrictions on phone calls via a crafted app that sends direct requests to the daemon.	2013-09-19	4.3	CVE-2013-5156
apple -- iphone_os	The Twitter subsystem in Apple iOS before 7 does not require API conformity for access to Twitter daemon interfaces, which allows attackers to post Tweets via a crafted app that sends direct requests to the daemon.	2013-09-19	4.3	CVE-2013-5157
apple -- iphone_os	WebKit in Apple iOS before 7 allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive information about use of the window.webkitRequestAnimationFrame API via an IFRAME element.	2013-09-19	4.3	CVE-2013-5159
chamanet -- chamacargo	Cross-site scripting (XSS) vulnerability in ChamaNet ChamaCargo 7.0000 and earlier allows remote attackers to inject arbitrary web script or HTML via	2013-09-16	4.3	CVE-2013-4704

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	unspecified vectors.			
cisco -- nx-os	The regex engine in the BGP implementation in Cisco NX-OS, when a complex regular expression is configured for inbound routes, allows remote attackers to cause a denial of service (device reload) via a crafted AS path set, aka Bug ID CSCuf49554.	2013-09-19	5.4	CVE-2013-1121
cisco -- socialminer	The gadget implementation in Cisco SocialMiner does not properly restrict the content of GET requests, which allows remote attackers to obtain sensitive information by reading (1) web-server access logs, (2) web-server Referer logs, or (3) the browser history, aka Bug ID CSCuh74125.	2013-09-13	5.0	CVE-2013-5489
cisco -- virtualization_experience_client_6000	The diagnostic module in the firmware on Cisco Virtualization Experience Client 6000 devices allows local users to bypass intended access restrictions and execute arbitrary commands via unspecified vectors, aka Bug ID CSCug68407.	2013-09-13	6.8	CVE-2013-5493
cisco -- unified_meetingplace	Cross-site request forgery (CSRF) vulnerability in the web framework in Cisco Unified MeetingPlace Solution, as used in Unified MeetingPlace Web Conferencing and Unified MeetingPlace, allows remote attackers to hijack the authentication of arbitrary users, aka Bug IDs CSCui45209 and CSCui44674.	2013-09-16	6.8	CVE-2013-5494
cisco -- unified_meetingplace	Cross-site scripting (XSS) vulnerability in the web framework in the Application Server in Cisco Unified MeetingPlace allows remote attackers to inject arbitrary web script or HTML via an unspecified parameter, aka Bug ID CSCui44681.	2013-09-16	4.3	CVE-2013-5495
cisco -- nx-os	Open Network Environment Platform (ONEP) in Cisco NX-OS allows remote authenticated users to cause a denial of service (network-element reload) via a crafted packet, aka Bug ID CSCui51551.	2013-09-16	6.3	CVE-2013-5496
cisco -- intrusion_prevention_system	The authentication manager process in the web framework in Cisco Intrusion Prevention System (IPS) does not properly handle user tokens, which allows remote attackers to cause a denial of service (intermittent MainApp hang) via a crafted management-interface connection request, aka Bug ID CSCuf20148.	2013-09-19	4.3	CVE-2013-5497
djangoproject -- django	Directory traversal vulnerability in Django 1.4.x before 1.4.7, 1.5.x before 1.5.3, and 1.6.x before 1.6 beta 3 allows remote attackers to read arbitrary files via a file path in the ALLOWED_INCLUDE_ROOTS setting followed by a .. (dot dot) in a ssi template tag.	2013-09-16	5.0	CVE-2013-4315

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
eucalyptus -- eucalyptus	Walrus in Eucalyptus before 3.2.2 allows remote attackers to cause a denial of service (memory, thread, and CPU consumption) via a crafted XML message containing a DTD, as demonstrated by a bucket-logging request.	2013-09-17	4.3	CVE-2012-4067
eucalyptus -- eucalyptus	Walrus in Eucalyptus before 3.2.2 does not verify authorization for the GetBucketLoggingStatus, SetBucketLoggingStatus, and SetBucketVersioningStatus bucket operations, which allows remote authenticated users to bypass intended restrictions on (1) modifying the logging setting, (2) modifying the versioning setting, or (3) accessing activity logs via a request.	2013-09-17	5.5	CVE-2013-2296
eucalyptus -- eustore	Eucalyptus EuStore sets a blank root password in the default configuration of EMI 3868652036, EMI 0400376721, EMI 2425352071, and EMI 1347115203, which allows local users to gain privileges via unspecified vectors, a related issue to CVE-2013-2069.	2013-09-17	6.9	CVE-2013-2297
eucalyptus -- eucalyptus	The gather log service in Eucalyptus before 3.3.1 allows remote attackers to read log files via an unspecified request to the (1) Cluster Controller (CC) or (2) Node Controller (NC) component.	2013-09-17	4.3	CVE-2013-4766
exactcode -- exactimage	econvert in ExactImage 0.8.9 and earlier does not properly initialize the setjmp variable, which allows context-dependent users to cause a denial of service (crash) via a crafted image file.	2013-09-16	4.3	CVE-2013-1441
ibm -- spss_analytical_decision_management	Cross-site scripting (XSS) vulnerability in IBM SPSS Analytical Decision Management 6.1 before IF1, 6.2 before IF1, and 7.0 before FP1 IF6 allows remote attackers to inject arbitrary web script or HTML via a crafted link.	2013-09-16	4.3	CVE-2013-4047
juniper -- ive_os	Multiple cross-site scripting (XSS) vulnerabilities in Juniper Junos Pulse Secure Access Service (aka SSL VPN) with IVE OS 7.1 before 7.1r15, 7.2 before 7.2r11, 7.3 before 7.3r6, and 7.4 before 7.4r3 allow (1) remote attackers to inject arbitrary web script or HTML via vectors involving login pages, and allow (2) remote authenticated users to inject arbitrary web script or HTML via vectors involving a support page.	2013-09-13	4.3	CVE-2013-5649
juniper -- junos_pulse_access_control_service	Junos Pulse Secure Access Service (IVE) 7.1 before 7.1r5, 7.2 before 7.2r10, 7.3 before 7.3r6, and 7.4 before 7.4r3 and Junos Pulse Access Control Service (UAC) 4.1 before 4.1r8.1, 4.2 before 4.2r5, 4.3 before 4.3r6 and 4.4 before 4.4r3, when a	2013-09-16	5.4	CVE-2013-5650

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	hardware SSL acceleration card is enabled, allows remote attackers to cause a denial of service (device hang) via a crafted packet.			
kde -- kde-workspace	KDE-Workspace 4.10.5 and earlier does not properly handle the return value of the glibc 2.17 crypt and pw_encrypt functions, which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via (1) an invalid salt or a (2) DES or (3) MD5 encrypted password, when FIPS-140 is enable, to KDM or an (4) invalid password to KCheckPass.	2013-09-16	5.0	CVE-2013-4132
konstanty_bialkowski -- libmodplug	Integer overflow in the abc_set_parts function in load_abc.cpp in libmodplug 0.8.8.4 and earlier allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted P header in an ABC file, which triggers a heap-based buffer overflow.	2013-09-16	6.8	CVE-2013-4233
konstanty_bialkowski -- libmodplug	Multiple heap-based buffer overflows in the (1) abc_MIDI_drum and (2) abc_MIDI_gchord functions in load_abc.cpp in libmodplug 0.8.8.4 and earlier allow remote attackers to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via a crafted ABC.	2013-09-16	6.8	CVE-2013-4234
libraw -- libraw	The "faster LJPEG decoder" in libraw 0.13.x, 0.14.x, and 0.15.x before 0.15.4 allows context-dependent attackers cause a denial of service (NULL pointer dereference) via a crafted photo file.	2013-09-16	4.3	CVE-2013-1439
linux -- linux_kernel	Multiple array index errors in drivers/hid/hid-core.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11 allow physically proximate attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a crafted device that provides an invalid Report ID.	2013-09-16	6.2	CVE-2013-2888
linux -- linux_kernel	drivers/hid/hid-zpff.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_ZEROPLUS is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	2013-09-16	4.7	CVE-2013-2889
linux -- linux_kernel	drivers/hid/hid-sony.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SONY is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	2013-09-16	4.7	CVE-2013-2890

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
linux -- linux_kernel	drivers/hid/hid-steelseries.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_STEELSERIES is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	2013-09-16	4.7	CVE-2013-2891
linux -- linux_kernel	drivers/hid/hid-pl.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_PANTHERLORD is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	2013-09-16	4.7	CVE-2013-2892
linux -- linux_kernel	The Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_LOGITECH_FF, CONFIG_LOGIG940_FF, or CONFIG_LOGIWHEELS_FF is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device, related to (1) drivers/hid/hid-lgff.c, (2) drivers/hid/hid-lg3ff.c, and (3) drivers/hid/hid-lg4ff.c.	2013-09-16	4.7	CVE-2013-2893
linux -- linux_kernel	drivers/hid/hid-lenovo-tpkbd.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_LENOVO_TPKBD is enabled, allows physically proximate attackers to cause a denial of service (heap-based out-of-bounds write) via a crafted device.	2013-09-16	4.7	CVE-2013-2894
linux -- linux_kernel	drivers/hid/hid-logitech-dj.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_LOGITECH_DJ is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) or obtain sensitive information from kernel memory via a crafted device.	2013-09-16	5.4	CVE-2013-2895
linux -- linux_kernel	drivers/hid/hid-ntrig.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_NTRIG is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) via a crafted device.	2013-09-16	4.7	CVE-2013-2896
linux -- linux_kernel	Multiple array index errors in drivers/hid/hid-multitouch.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_MULTITOUCH is enabled, allow physically proximate attackers	2013-09-16	4.7	CVE-2013-2897

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	to cause a denial of service (heap memory corruption, or NULL pointer dereference and OOPS) via a crafted device.			
linux -- linux_kernel	drivers/hid/hid-picolcd_core.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_PICOLCD is enabled, allows physically proximate attackers to cause a denial of service (NULL pointer dereference and OOPS) via a crafted device.	2013-09-16	4.7	CVE-2013-2899
moodle -- moodle	repository/s3/S3.php in the Amazon S3 library in Moodle through 2.2.11, 2.3.x before 2.3.9, 2.4.x before 2.4.6, and 2.5.x before 2.5.2 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, related to an incorrect CURLOPT_SSL_VERIFYHOST value.	2013-09-16	5.8	CVE-2012-6087
moodle -- moodle	Multiple cross-site scripting (XSS) vulnerabilities in Moodle through 2.2.11, 2.3.x before 2.3.9, 2.4.x before 2.4.6, and 2.5.x before 2.5.2 allow remote attackers to inject arbitrary web script or HTML via a crafted blog link within an RSS feed.	2013-09-16	4.3	CVE-2013-4341
mozilla -- firefox	Integer overflow in the drawLineLoop function in the libGLESv2 library in Almost Native Graphics Layer Engine (ANGLE), as used in Mozilla Firefox before 24.0 and SeaMonkey before 2.21, allows remote attackers to execute arbitrary code via a crafted web site.	2013-09-18	6.8	CVE-2013-1721
mozilla -- firefox	The NativeKey widget in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21 processes key messages after destruction by a dispatched event listener, which allows remote attackers to cause a denial of service (application crash) by leveraging incorrect event usage after widget-memory reallocation.	2013-09-18	4.3	CVE-2013-1723
mozilla -- firefox	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not ensure that initialization occurs for JavaScript objects with compartments, which allows remote attackers to execute arbitrary code by leveraging incorrect scope handling.	2013-09-18	6.8	CVE-2013-1725
mozilla -- firefox	Mozilla Updater in Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9,	2013-09-18	6.2	CVE-2013-1726

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 does not ensure exclusive access to a MAR file, which allows local users to gain privileges by creating a Trojan horse file after MAR signature verification but before MAR use.			
mozilla -- firefox	Mozilla Firefox before 24.0 on Android allows attackers to bypass the Same Origin Policy, and consequently conduct cross-site scripting (XSS) attacks or obtain password or cookie information, by using a symlink in conjunction with a file: URL for a local file.	2013-09-18	4.0	CVE-2013-1727
mozilla -- firefox	The IonMonkey JavaScript engine in Mozilla Firefox before 24.0, Thunderbird before 24.0, and SeaMonkey before 2.21, when Valgrind mode is used, does not properly initialize memory, which makes it easier for remote attackers to obtain sensitive information via unspecified vectors.	2013-09-18	4.3	CVE-2013-1728
mozilla -- firefox	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not properly handle movement of XBL-backed nodes between documents, which allows remote attackers to execute arbitrary code or cause a denial of service (JavaScript compartment mismatch, or assertion failure and application exit) via a crafted web site.	2013-09-18	6.8	CVE-2013-1730
mozilla -- firefox	Mozilla Firefox before 24.0, Firefox ESR 17.x before 17.0.9, Thunderbird before 24.0, Thunderbird ESR 17.x before 17.0.9, and SeaMonkey before 2.21 do not properly identify the "this" object during use of user-defined getter methods on DOM proxies, which might allow remote attackers to bypass intended access restrictions via vectors involving an expando object.	2013-09-18	5.0	CVE-2013-1737
openstack -- compute	OpenStack Compute (Nova) before 2013.1.3 and Havana before havana-2 does not properly enforce the os-flavor-access:is_public property, which allows remote authenticated users to obtain sensitive information (flavor properties), boot arbitrary flavors, and possibly have other unspecified impacts by guessing the flavor id.	2013-09-16	6.0	CVE-2013-2256
openstack -- compute	The security group extension in OpenStack Compute (Nova) Grizzly 2013.1.3, Havana before havana-3, and earlier allows remote attackers to cause a denial of	2013-09-16	4.3	CVE-2013-4179

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	service (resource consumption and crash) via an XML Entity Expansion (XEE) attack. NOTE: this issue is due to an incomplete fix for CVE-2013-1664.			
openstack -- compute	The (1) backup (api/contrib/backups.py) and (2) volume transfer (contrib/volume_transfer.py) APIs in OpenStack Cinder Grizzly 2013.1.3 and earlier allows remote attackers to cause a denial of service (resource consumption and crash) via an XML Entity Expansion (XEE) attack. NOTE: this issue is due to an incomplete fix for CVE-2013-1664.	2013-09-16	4.3	CVE-2013-4202
php -- php	The SOAP parser in PHP before 5.3.22 and 5.4.x before 5.4.12 allows remote attackers to read arbitrary files via a SOAP WSDL file containing an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue in the soap_xmlParseFile and soap_xmlParseMemory functions.	2013-09-16	4.3	CVE-2013-1824
redhat -- openstack	The (1) power and (2) ipmi_boot actions in the HostController in Foreman before 1.2.2 allow remote attackers to cause a denial of service (memory consumption) via unspecified input that is converted to a symbol.	2013-09-16	5.0	CVE-2013-4180
redhat -- enterprise_virtualization	Cross-site scripting (XSS) vulnerability in the addAlert function in the RedirectServlet servlet in oVirt Engine and Red Hat Enterprise Virtualization Manager (RHEV-M), as used in Red Hat Enterprise Virtualization 3 and 3.2, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2013-09-16	4.3	CVE-2013-4181
sap -- netweaver	Directory traversal vulnerability in SAP NetWeaver 7.x allows remote attackers to read arbitrary files via unspecified vectors.	2013-09-16	5.0	CVE-2013-5751
slickremix -- design_approval_system_plugin	Cross-site scripting (XSS) vulnerability in admin/walkthrough/walkthrough.php in the Design Approval System plugin before 3.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the step parameter.	2013-09-17	4.3	CVE-2013-5711
squid-cache -- squid	client_side_request.cc in Squid 3.2.x before 3.2.13 and 3.3.x before 3.3.8 allows remote attackers to cause a denial of service via a crafted port number in a HTTP Host header.	2013-09-16	5.0	CVE-2013-4123
subnet -- substation_server	The DNP3 Slave service in SUBNET Solutions SubSTATION Server 2.7.0033 and 2.8.0106 allows remote attackers to cause a denial of service (unhandled	2013-09-17	4.3	CVE-2013-2788

High Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	exception and process crash) via unspecified vectors.			
wireshark -- wireshark	The Bluetooth HCI ACL dissector in Wireshark 1.10.x before 1.10.2 does not properly maintain a certain free list, which allows remote attackers to cause a denial of service (application crash) via a crafted packet that is not properly handled by the wmem_block_alloc function in epan/wmem/wmem_allocator_block.c.	2013-09-16	4.3	CVE-2013-5717
wireshark -- wireshark	The dissect_nbap_T_dCH_ID function in epan/dissectors/packet-nbap.c in the NBAP dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 does not restrict the dch_id value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	2013-09-16	4.3	CVE-2013-5718
wireshark -- wireshark	epan/dissectors/packet-assa_r3.c in the ASSA R3 dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.	2013-09-16	4.3	CVE-2013-5719
wireshark -- wireshark	Buffer overflow in the RTPS dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 allows remote attackers to cause a denial of service (application crash) via a crafted packet.	2013-09-16	4.3	CVE-2013-5720
wireshark -- wireshark	The dissect_mq_rr function in epan/dissectors/packet-mq.c in the MQ dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 does not properly determine when to enter a certain loop, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.	2013-09-16	4.3	CVE-2013-5721
wireshark -- wireshark	Unspecified vulnerability in the LDAP dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 allows remote attackers to cause a denial of service (application crash) via a crafted packet.	2013-09-16	4.3	CVE-2013-5722

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
Back to top				
ansibleworks -- ansible	runner/connection_plugins/ssh.py in Ansible before 1.2.3, when using ControlPersist, allows local users to redirect a ssh session via a symlink attack on a socket file with a predictable name in /tmp/.	2013-09-16	1.9	CVE-2013-4259

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
ansibleworks -- ansible	lib/ansible/playbook/__init__.py in Ansible 1.2.x before 1.2.3, when playbook does not run due to an error, allows local users to overwrite arbitrary files via a symlink attack on a retry file with a predictable name in /var/tmp/ansible/.	2013-09-16	3.3	CVE-2013-4260
apache -- subversion	Svnserve in Apache Subversion 1.4.0 through 1.7.12 and 1.8.0 through 1.8.1 allows local users to overwrite arbitrary files or kill arbitrary processes via a symlink attack on the file specified by the --pid-file option.	2013-09-16	3.3	CVE-2013-4277
apple -- mac_os_x	mdmclient in Mobile Device Management in Apple Mac OS X before 10.8.5 places a password on the command line, which allows local users to obtain sensitive information by listing the process.	2013-09-16	2.1	CVE-2013-1030
apple -- mac_os_x	Power Management in Apple Mac OS X before 10.8.5 does not properly perform locking upon occurrences of a power assertion, which allows physically proximate attackers to bypass intended access restrictions by visiting an unattended workstation on which a locking failure had prevented the startup of the screen saver.	2013-09-16	3.3	CVE-2013-1031
apple -- iphone_os	IOKit in Apple iOS before 7 allows attackers to send user-interface events to the foreground app by leveraging control over a background app and using the (1) task-completion API or (2) VoIP API.	2013-09-19	2.6	CVE-2013-5137
apple -- iphone_os	IOCatalogue in IOKitUser in Apple iOS before 7 allows attackers to cause a denial of service (NULL pointer dereference and device crash) via a crafted application.	2013-09-19	1.9	CVE-2013-5138
apple -- iphone_os	kextd in Kext Management in Apple iOS before 7 does not properly verify authorization for IPC messages, which allows local users to (1) load or (2) unload kernel extensions via a crafted message.	2013-09-19	1.9	CVE-2013-5145
apple -- iphone_os	The history-clearing feature in Safari in Apple iOS before 7 does not clear the back/forward history of an open tab, which allows physically proximate attackers to obtain sensitive information by leveraging an unattended workstation.	2013-09-19	1.9	CVE-2013-5150
apple -- iphone_os	Springboard in Apple iOS before 7 does not properly manage the lock state in Lost Mode, which allows physically proximate attackers to read notifications via unspecified vectors.	2013-09-19	2.1	CVE-2013-5153
apple -- iphone_os	The Social subsystem in Apple iOS before 7 does not properly restrict access to	2013-09-19	2.1	CVE-2013-5158

Low Vulnerabilities				
Primary Vendor -- Product	**Description**	**Published**	**CVSS Score**	**Source & Patch Info**
	the cache of Twitter icons, which allows physically proximate attackers to obtain sensitive information about recent Twitter interaction via unspecified vectors.			
ibm -- spss_analytical_decision_management	Cross-site scripting (XSS) vulnerability in IBM SPSS Analytical Decision Management 6.1 before IF1, 6.2 before IF1, and 7.0 before FP1 IF6 allows remote authenticated users to inject arbitrary web script or HTML via vectors involving addition of script to a page.	2013-09-16	3.5	CVE-2013-4048
linux -- linux_kernel	drivers/hid/hid-sensor-hub.c in the Human Interface Device (HID) subsystem in the Linux kernel through 3.11, when CONFIG_HID_SENSOR_HUB is enabled, allows physically proximate attackers to obtain sensitive information from kernel memory via a crafted device.	2013-09-16	1.9	CVE-2013-2898
mozilla -- firefox	The WebGL implementation in Mozilla Firefox before 24.0, when NVIDIA graphics drivers are used on Mac OS X, allows remote attackers to obtain desktop-screenshot data by reading from a CANVAS element.	2013-09-18	2.6	CVE-2013-1729
openstack -- compute	The clear_volume function in LVMVolumeDriver driver in OpenStack Cinder 2013.1.1 through 2013.1.2 does not properly clear data when deleting a snapshot, which allows local users to obtain sensitive information via unspecified vectors.	2013-09-16	2.1	CVE-2013-4183
openstack -- compute	The "create an instance" API in OpenStack Compute (Nova) Folsom, Grizzly, and Havana does not properly enforce the os-flavor-access:is_public property, which allows remote authenticated users to boot arbitrary flavors by guessing the flavor id. NOTE: this issue is due to an incomplete fix for CVE-2013-2256.	2013-09-16	3.5	CVE-2013-4278