Vulnerability Summary for the Week of June 9, 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**
aas9 -- zerocms	SQL injection vulnerability in zero_view_article.php in ZeroCMS 1.0 allows remote attackers to execute arbitrary SQL commands via the article_id parameter.	2014-06-11	7.5	CVE-2014-4034
adobe -- adobe_air	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0535.	2014-06-11	7.5	CVE-2014-0534
adobe -- adobe_air	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0534.	2014-06-11	7.5	CVE-2014-0535

adobe -- adobe_air	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	2014-06-11	10.0	CVE-2014-0536
condor_project -- condor	The standard universe shadow (condor_shadow.std) component in Condor 7.7.3 through 7.7.6, 7.8.0 before 7.8.5, and 7.9.0 does no properly check privileges, which allows remote attackers to gain privileges via a crafted standard universe job.	2014-06-06	10.0	CVE-2012-5390
directfb -- directfb	Multiple integer signedness errors in the Dispatch_Write function in proxy/dispatcher/idirectfbsurface_dispatcher.c in DirectFB 1.4.13 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the Voodoo interface, which triggers a stack-based buffer overflow.	2014-06-11	10.0	CVE-2014-2977
directfb -- directfb	The Dispatch_Write function in proxy/dispatcher/idirectfbsurface_dispatcher.c in DirectFB 1.4.4 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via the Voodoo interface, which triggers an out-of-bounds write.	2014-06-11	10.0	CVE-2014-2978
emc -- documentum_content_server	EMC Documentum Content Server before 6.7 SP1 P28, 6.7 SP2 before P14, 7.0 before P15, and 7.1 before P05 allows remote authenticated users to obtain super-user privileges for system-object creation, and bypass intended restrictions on data access and server actions, via unspecified vectors.	2014-06-08	8.5	CVE-2014-2506
emc -- documentum_content_server	EMC Documentum Content Server before 6.7 SP1 P28, 6.7 SP2 before P14, 7.0 before P15, and 7.1 before P05 allows remote authenticated users to execute arbitrary commands via shell	2014-06-08	8.5	CVE-2014-2507

	metacharacters in arguments to unspecified methods.			
emc -- documentum_content_server	EMC Documentum Content Server before 6.7 SP1 P28, 6.7 SP2 before P14, 7.0 before P15, and 7.1 before P05 allows remote authenticated users to conduct Documentum Query Language (DQL) injection attacks and bypass intended restrictions on database actions via vectors involving DQL hints.	2014-06-08	7.5	CVE-2014-2508
google -- chrome	Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/child_thread.cc in the filesystem API in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a Blink shutdown.	2014-06-11	7.5	CVE-2014-3154
google -- chrome	Buffer overflow in the clipboard implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unexpected bitmap data, related to content/renderer/renderer_clipboard_client.cc and content/renderer/webclipboard_impl.cc.	2014-06-11	7.5	CVE-2014-3156
google -- chrome	Heap-based buffer overflow in the FFmpegVideoDecoder::GetVideoBuffer function in media/filters/ffmpeg_video_decoder.cc in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging VideoFrame data structures that are too small for proper interaction with an underlying FFmpeg library.	2014-06-11	7.5	CVE-2014-3157
jojocms -- jojo-cms	SQL injection vulnerability in the checkEmailFormat function in plugins/jojo_core/classes/Jojo.php in Jojo before 1.2.2 allows remote attackers to execute arbitrary SQL commands via the X-Forwarded-	2014-06-09	7.5	CVE-2013-3081

	For HTTP header to /articles/test/.			
libav -- libav	Multiple unspecified vulnerabilities in Libav before 0.8.12 allow remote attackers to have unknown impact and vectors.	2014-06-06	10.0	CVE-2014-3984
mark_evans -- dragonfly_gem	The Dragonfly gem 0.7 before 0.8.6 and 0.9.x before 0.9.13 for Ruby, when used with Ruby on Rails, allows remote attackers to execute arbitrary code via a crafted request.	2014-06-09	7.5	CVE-2013-1756
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-2014-1775, CVE-2014-1779, CVE-2014-1799, CVE-2014-1803, and CVE-2014-2757.	2014-06-11	9.3	CVE-2014-0282
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.	2014-06-11	9.3	CVE-2014-1769
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-1772
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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	2014-06-11	9.3	CVE-2014-1773

	Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.			
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1788 and CVE-2014-2754.	2014-06-11	9.3	CVE-2014-1774
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-2014-0282, CVE-2014-1779, CVE-2014-1799, CVE-2014-1803, and CVE-2014-2757.	2014-06-11	9.3	CVE-2014-1775
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-2014-0282, CVE-2014-1775, CVE-2014-1799, CVE-2014-1803, and CVE-2014-2757.	2014-06-11	9.3	CVE-2014-1779
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-1780

microsoft -- internet_explorer	Microsoft Internet Explorer 8 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-2014-1792, CVE-2014-1804, and CVE-2014-2770.	2014-06-11	9.3	CVE-2014-1781
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1769, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.	2014-06-11	9.3	CVE-2014-1782
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-1783
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-1784
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	2014-06-11	9.3	CVE-2014-1785

	crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.			
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-1786
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1774 and CVE-2014-2754.	2014-06-11	9.3	CVE-2014-1788
microsoft -- internet_explorer	Microsoft Internet Explorer 10 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-2014-1790.	2014-06-11	9.3	CVE-2014-1789
microsoft -- internet_explorer	Microsoft Internet Explorer 10 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-2014-1789.	2014-06-11	9.3	CVE-2014-1790
microsoft -- internet_explorer	Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via	2014-06-11	9.3	CVE-2014-1791

	a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability."			
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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-2014-1781, CVE-2014-1804, and CVE-2014-2770.	2014-06-11	9.3	CVE-2014-1792
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-1794
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-1795
microsoft -- internet_explorer	Microsoft Internet Explorer 6 and 8 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."	2014-06-11	9.3	CVE-2014-1796
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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	2014-06-11	9.3	CVE-2014-1797

	vulnerability than CVE-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.			
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-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1803, and CVE-2014-2757.	2014-06-11	9.3	CVE-2014-1799
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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."	2014-06-11	9.3	CVE-2014-1800
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-1802
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-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, and CVE-2014-2757.	2014-06-11	9.3	CVE-2014-1803
microsoft -- internet_explorer	Microsoft Internet Explorer 8 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory	2014-06-11	9.3	CVE-2014-1804

	Corruption Vulnerability," a different vulnerability than CVE-2014-1781, CVE-2014-1792, and CVE-2014-2770.			
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-1805
microsoft -- windows_7	usp10.dll in Uniscribe (aka the Unicode Script Processor) 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, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted EMF+ record in a font file, aka "Unicode Scripts Processor Vulnerability."	2014-06-11	9.3	CVE-2014-1817
microsoft -- windows_7	GDI+ 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, Windows RT Gold and 8.1, Office 2007 SP3 and 2010 SP1 and SP2, Live Meeting 2007 Console, Lync 2010 and 2013, Lync 2010 Attendee, and Lync Basic 2013 allows remote attackers to execute arbitrary code via a crafted EMF+ record in an image file, aka "GDI+ Image Parsing Vulnerability."	2014-06-11	9.3	CVE-2014-1818
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a	2014-06-11	9.3	CVE-2014-2753

	denial of service (memory corruption) via a crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.			
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1774 and CVE-2014-1788.	2014-06-11	9.3	CVE-2014-2754
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2760, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.	2014-06-11	9.3	CVE-2014-2755
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2763, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-2756
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-2014-0282, CVE-2014-1775, CVE-2014-1779, CVE-2014-1799, and CVE-	2014-06-11	9.3	CVE-2014-2757

	2014-1803.			
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2759, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-2758
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2765, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-2759
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2761, CVE-2014-2772, and CVE-2014-2776.	2014-06-11	9.3	CVE-2014-2760
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2772, and CVE-2014-2776.	2014-06-11	9.3	CVE-2014-2761

microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2764, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-2763
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2769, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-2764
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2766, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-2765
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-2014-2775.	2014-06-11	9.3	CVE-2014-2766
microsoft --	Microsoft Internet Explorer 6 and 7 allows	2014-06-11	9.3	CVE-2014-2767

internet_explorer	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."			
microsoft -- internet_explorer	Microsoft Internet Explorer 6 through 8 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-2014-2773.	2014-06-11	9.3	CVE-2014-2768
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2771.	2014-06-11	9.3	CVE-2014-2769
microsoft -- internet_explorer	Microsoft Internet Explorer 8 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-2014-1781, CVE-2014-1792, and CVE-2014-1804.	2014-06-11	9.3	CVE-2014-2770
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 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-2014-1772, CVE-2014-1780, CVE-2014-1794, CVE-2014-1797, CVE-2014-1802, CVE-2014-2756, CVE-2014-2763, CVE-2014-2764, and CVE-2014-2769.	2014-06-11	9.3	CVE-2014-2771
microsoft -- internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a	2014-06-11	9.3	CVE-2014-2772

	crafted web site, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2776.			
microsoft -- internet_explorer	Microsoft Internet Explorer 6 through 8 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-2014-2768.	2014-06-11	9.3	CVE-2014-2773
microsoft -- internet_explorer	Microsoft Internet Explorer 9 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-2014-1773, CVE-2014-1783, CVE-2014-1784, CVE-2014-1786, CVE-2014-1795, CVE-2014-1805, CVE-2014-2758, CVE-2014-2759, CVE-2014-2765, and CVE-2014-2766.	2014-06-11	9.3	CVE-2014-2775
microsoft -- internet_explorer	Microsoft Internet Explorer 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-2014-1769, CVE-2014-1782, CVE-2014-1785, CVE-2014-2753, CVE-2014-2755, CVE-2014-2760, CVE-2014-2761, and CVE-2014-2772.	2014-06-11	9.3	CVE-2014-2776
microsoft -- internet_explorer	Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with increased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-1778.	2014-06-11	7.5	CVE-2014-2777
microsoft --	Microsoft Word 2007 SP3 and Office	2014-06-11	9.3	CVE-2014-2778

office_compatibility_pack	Compatibility Pack SP3 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted embedded font in a (1) .doc or (2) .docx document, aka "Embedded Font Vulnerability."			
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2014-06-11	10.0	CVE-2014-1533
mozilla -- firefox	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 30.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	2014-06-11	10.0	CVE-2014-1534
mozilla -- firefox	The PropertyProvider::FindJustificationRange function in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via unspecified vectors.	2014-06-11	10.0	CVE-2014-1536
mozilla -- firefox	Use-after-free vulnerability in the mozilla::dom::workers::WorkerPrivateParent function in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.	2014-06-11	10.0	CVE-2014-1537
mozilla -- firefox	Use-after-free vulnerability in the nsTextEditRules::CreateMozBR function in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.	2014-06-11	10.0	CVE-2014-1538
mozilla -- firefox	Use-after-free vulnerability in the nsEventListenerManager::CompileEventHandlerI	2014-06-11	9.3	CVE-2014-1540

	nternal function in the Event Listener Manager in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via crafted web content.			
mozilla -- firefox	Use-after-free vulnerability in the RefreshDriverTimer::TickDriver function in the SMIL Animation Controller in Mozilla Firefox before 30.0, Firefox ESR 24.x before 24.6, and Thunderbird before 24.6 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via crafted web content.	2014-06-11	10.0	CVE-2014-1541
mozilla -- firefox	Multiple heap-based buffer overflows in the navigator.getGamepads function in the Gamepad API in Mozilla Firefox before 30.0 allow remote attackers to execute arbitrary code by using non-contiguous axes with a (1) physical or (2) virtual Gamepad device.	2014-06-11	7.5	CVE-2014-1543
mozilla -- netscape_portable_runtime	Mozilla Netscape Portable Runtime (NSPR) before 4.10.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via vectors involving the sprintf and console functions.	2014-06-11	10.0	CVE-2014-1545
mplayer2 -- mplayer2	Stack-based buffer overflow in the sub_read_line_sami function in subreader.c in MPlayer, as used in SMPlayer 0.6.9, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long string in a SAMI subtitle file.	2014-06-11	9.3	CVE-2011-3625
myheritage -- sequeryobject_activex_control	Multiple array index errors in the MyHeritage SEQueryObject ActiveX control (SearchEngineQuery.dll) 1.0.2.0 allow remote attackers to execute arbitrary code via the (1) seTokensArray, or (2) seTokensValuesArray parameter to the AddTokens method; (3) seLastNameTokensArray parameter to the AddLastNameTokens method; (4)	2014-06-06	9.3	CVE-2013-2602

	seFrameIdArray, (5) seSourceIdArray, (6) seHasBreakdownArray, (7) seIsIndexedArray, (8) seAllConcatArray, (9) seRefererURLArray, or (10) seMandatoryFieldsArray parameter to the AddMultipleSearches method; (11) seSourceIdArray, (12) seIsIndexedArray, (13) seAllConcatArray, (14) seRefererURLArray, (15) seQATestsArray, (16) seAllSourceIDsArray, (17) seAllSourceTitlesArray, (18) seMandatoryFieldsArray, or (19) seAllSourceRootURLArray parameter to the TestYourself method.			
offis -- dcmtk	(1) movescu.cc and (2) storescp.cc in dcmnet/apps/, (3) dcmnet/libsrc/scp.cc, (4) dcmwlm/libsrc/wlmactmg.cc, (5) dcmprscp.cc and (6) dcmpsrcv.cc in dcmpstat/apps/, (7) dcmpstat/tests/msgserv.cc, and (8) dcmqrdb/apps/dcmqrscp.cc in DCMTK 3.6.1 and earlier does not check the return value of the setuid system call, which allows local users to gain privileges by creating a large number of processes.	2014-06-10	7.2	CVE-2013-6825
redhat -- enterprise_mrg	The futex_requeue function in kernel/futex.c in the Linux kernel through 3.14.5 does not ensure that calls have two different futex addresses, which allows local users to gain privileges via a crafted FUTEX_REQUEUE command that facilitates unsafe waiter modification.	2014-06-07	7.2	CVE-2014-3153
rocketsoftware -- rocket_servergraph	The userRequest servlet in the Admin Center for Tivoli Storage Manager in Rocket Servergraph allows remote attackers to execute arbitrary commands via a (1) auth, (2) auth_session, (3) auth_simple, (4) add, (5) add_flat, (6) remove, (7) set_pwd, (8) add_permissions, (9) revoke_permissions, (10) runAsync, or (11) tsmRequest command.	2014-06-11	10.0	CVE-2014-3915
samsung -- ipolis_device_manager	Samsung iPOLiS Device Manager before 1.8.7 allow remote attackers to execute arbitrary code via unspecified values to the (1) Start, (2)	2014-06-11	9.3	CVE-2014-3911

	ChangeControlLocalName, (3) DeleteDeviceProfile, (4) FrameAdvanceReader, or other unknown method in the XNSSDKDEVICE.XnsSdkDeviceCtrlForIpInstaller.1 ActiveX control.			
sap -- netweaver	The System Landscape Directory (SLD) in SAP NetWeaver allows remote attackers to modify information via vectors related to adding a system.	2014-06-09	7.5	CVE-2014-4003
vinay_sajip -- python-gnupg	python-gnupg before 0.3.5 allows context-dependent attackers to execute arbitrary commands via shell metacharacters in unspecified vectors.	2014-06-09	7.5	CVE-2013-7323

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
adobe -- adobe_air	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0532 and CVE-2014-0533.	2014-06-11	4.3	CVE-2014-0531
adobe -- adobe_air	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before	2014-06-11	4.3	CVE-2014-0532

	11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0533.			
adobe -- adobe_air	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0532.	2014-06-11	4.3	CVE-2014-0533
autocomplete_widgets_project -- autocomplete_widgets	The autocomplete callback in Autocomplete Widgets for Text and Number Fields (autocomplete_widgets) module 6.x-1.x before 6.x-1.4 and 7.x-1.x before 7.x-1.0-rc1 does not properly handle node permissions, which allows remote authenticated users to obtain sensitive field values via unspecified vectors.	2014-06-09	4.0	CVE-2013-1973
bestsoftinc -- advance_hotel_booking_system	Cross-site scripting (XSS) vulnerability in booking_details.php in Best Soft Inc. (BSI) Advance Hotel Booking System 2.0 allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2014-06-11	4.3	CVE-2014-4035
castor_project -- castor	The default configuration for the Xerces SAX Parser in Castor before 1.3.3 allows context-dependent attackers to conduct XML External Entity (XXE) attacks via a crafted XML document.	2014-06-11	4.3	CVE-2014-3004
cisco -- unified_communications_domain_manager	The web framework in VOSS in Cisco Unified Communications Domain Manager (CDM) does not properly implement access control, which allows remote attackers to enumerate accounts by visiting an unspecified BVSMWeb web page, aka Bug IDs CSCun39619 and CSCun45572.	2014-06-08	5.0	CVE-2014-3278
cisco --	The web framework in VOSS in Cisco Unified	2014-06-08	5.0	CVE-2014-3281

unified_communications_domain_manager	Communications Domain Manager (CDM) does not properly implement access control, which allows remote attackers to obtain potentially sensitive user information by visiting an unspecified BVSMWeb web page, aka Bug IDs CSCun46071 and CSCun46101.			
cisco -- webex_meetings_server	The web framework in Cisco WebEx Meeting Server does not properly restrict the content of reply messages, which allows remote attackers to obtain sensitive information via a crafted URL, aka Bug IDs CSCuj81685, CSCuj81688, CSCuj81665, CSCuj81744, and CSCuj81661.	2014-06-08	5.0	CVE-2014-3286
cisco -- unified_communications_manager	SQL injection vulnerability in BulkViewFileContentsAction.java in the Java interface in Cisco Unified Communications Manager (Unified CM) allows remote authenticated users to execute arbitrary SQL commands via crafted filename parameters in a URL, aka Bug ID CSCuo17337.	2014-06-10	4.0	CVE-2014-3287
cisco -- content_security_management_appliance	Cross-site scripting (XSS) vulnerability in the web management interface in Cisco AsyncOS on the Email Security Appliance (ESA) 8.0, Web Security Appliance (WSA) 8.0 (.5 Hot Patch 1) and earlier, and Content Security Management Appliance (SMA) 8.3 and earlier allows remote attackers to inject arbitrary web script or HTML via a crafted parameter, as demonstrated by the date_range parameter to monitor/reports/overview on the IronPort ESA, aka Bug IDs CSCun07998, CSCun07844, and CSCun07888.	2014-06-10	4.3	CVE-2014-3289
cisco -- wireless_lan_controller	Cisco Wireless LAN Controller (WLC) devices allow remote attackers to cause a denial of service (NULL pointer dereference and device restart) via a zero value in Cisco Discovery Protocol packet data that is not properly handled during SNMP polling, aka Bug ID CSCuo12321.	2014-06-08	5.7	CVE-2014-3291
cisco -- unified_communica	The Real Time Monitoring Tool (RTMT) implementation in Cisco Unified Communications	2014-06-10	5.5	CVE-2014-3292

tions_manager	Manager (Unified CM) allows remote authenticated users to (1) read or (2) delete arbitrary files via a crafted URL, aka Bug IDs CSCuo17302 and CSCuo17199.			
cisco -- webex_meetings_server	Cisco WebEx Meeting Server does not properly restrict the content of URLs, which allows remote authenticated users to obtain sensitive information by reading (1) web-server access logs, (2) web-server Referer logs, or (3) the browser history, aka Bug ID CSCuj81691.	2014-06-10	4.0	CVE-2014-3294
ckeditor -- fckeditor	Cross-site scripting (XSS) vulnerability in editor/dialog/fck_spellerpages/spellerpages/server-scripts/spellchecker.php in FCKeditor before 2.6.11 and earlier allows remote attackers to inject arbitrary web script or HTML via an array key in the textinputs[] parameter, a different issue than CVE-2012-4000.	2014-06-11	4.3	CVE-2014-4037
cloudera -- cloudera_manager	Cloudera Manager before 4.8.3 and 5.x before 5.0.1 allows remote authenticated users to obtain sensitive configuration information via the API.	2014-06-10	4.0	CVE-2014-0220
conversion_ninja -- conversion_ninja	Cross-site scripting (XSS) vulnerability in the Conversion Ninja plugin for WordPress allows remote attackers to inject arbitrary web script or HTML via the id parameter to lp/index.php.	2014-06-10	4.3	CVE-2014-4017
corosync -- corosync	The init_nss_hash function in exec/totemcrypto.c in Corosync 2.0 before 2.3 does not properly initialize the HMAC key, which allows remote attackers to cause a denial of service (crash) via a crafted packet.	2014-06-06	5.0	CVE-2013-0250
daiki_ueno -- libfep	libfep 0.0.5 before 0.1.0 does not properly use UNIX domain sockets in the abstract namespace, which allows local users to gain privileges via unspecified vectors.	2014-06-11	4.6	CVE-2014-3980
ddsn -- cm3_acora_content_management_system	DDSN Interactive cm3 Acora CMS 6.0.6/1a, 6.0.2/1a, 5.5.7/12b, 5.5.0/1b-p1, and possibly other versions, does not include the HTTPOnly flag in a Set-Cookie header for an unspecified cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie.	2014-06-06	5.0	CVE-2013-4724

ddsn -- cm3_acora_content_management_system	DDSN Interactive cm3 Acora CMS 6.0.6/1a, 6.0.2/1a, 5.5.7/12b, 5.5.0/1b-p1, and possibly other versions, does not set the secure flag for an unspecified cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session.	2014-06-06	5.0	CVE-2013-4725
ddsn -- cm3_acora_content_management_system	DDSN Interactive cm3 Acora CMS 6.0.6/1a, 6.0.2/1a, 5.5.7/12b, 5.5.0/1b-p1, and possibly other versions, allows remote attackers to obtain sensitive information via a request to Admin/top.aspx.	2014-06-06	5.0	CVE-2013-4727
ddsn -- cm3_acora_content_management_system	DDSN Interactive cm3 Acora CMS 6.0.6/1a, 6.0.2/1a, 5.5.7/12b, 5.5.0/1b-p1, and possibly other versions, allows remote attackers to obtain sensitive information via a .. (dot dot) in the "l" parameter, which reveals the installation path in an error message.	2014-06-06	5.0	CVE-2013-4728
devexpress -- aspxfilemanager_control_for_webforms_and_mvc	Directory traversal vulnerability in the File Manager component in DevExpress ASPxFileManager Control for ASP.NET WebForms and MVC before 13.1.10 and 13.2.x before 13.2.9 allows remote authenticated users to read or write arbitrary files via a .. (dot dot) in the __EVENTARGUMENT parameter.	2014-06-06	6.5	CVE-2014-2575
dotclear -- dotclear	The dcXmlRpc::setUser method in nc/core/class.dc.xmlrpc.php in Dotclear before 2.6.3 allows remote attackers to bypass authentication via an empty password in an XML-RPC request.	2014-06-11	5.8	CVE-2014-3781
dotclear -- dotclear	Multiple incomplete blacklist vulnerabilities in the filemanager::isFileExclude method in the Media Manager in Dotclear before 2.6.3 allow remote authenticated users to execute arbitrary PHP code by uploading a file with a (1) double extension or (2) .php5, (3) .phtml, or some other PHP file extension.	2014-06-11	6.0	CVE-2014-3782
efrontlearning -- efront	Cross-site scripting (XSS) vulnerability in libraries/includes/personal/profile.php in Epignosis eFront 3.6.14.4 allows remote attackers to inject arbitrary web script or HTML via the surname	2014-06-11	4.3	CVE-2014-4033

	parameter to student.php.			
fail2ban -- fail2ban	The (1) dshield.conf, (2) mail-buffered.conf, (3) mynetwatchman.conf, and (4) mynetwatchman.conf actions in action.d/ in Fail2ban before 0.8.5 allows local users to write to arbitrary files via a symlink attack on temporary files with predictable names, as demonstrated by /tmp/fail2ban-mail.txt.	2014-06-10	4.7	CVE-2009-5023
fiyo -- fiyo_cms	Cross-site scripting (XSS) vulnerability in apps/app_comment/form_comment.php in Fiyo CMS 1.5.7 allows remote attackers to inject arbitrary web script or HTML via the Nama field.	2014-06-11	4.3	CVE-2014-4032
freebsd -- freebsd	The (1) execve and (2) fexecve system calls in the FreeBSD kernel 8.4 before p11, 9.1 before p14, 9.2 before p7, and 10.0 before p4 destroys the virtual memory address space and mappings for a process before all threads have terminated, which allows local users to cause a denial of service (triple-fault and system reboot) via a crafted system call, which triggers an invalid page table pointer dereference.	2014-06-10	4.9	CVE-2014-3880
gnu -- gnutls	The gnutls_x509_dn_oid_name function in lib/x509/common.c in GnuTLS 3.0 before 3.1.20 and 3.2.x before 3.2.10 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted X.509 certificate, related to a missing LDAP description for an OID when printing the DN.	2014-06-10	5.0	CVE-2014-3465
gomlab -- gom_media_player	GOM Media Player 2.2.57.5189 and earlier allows remote attackers to cause a denial of service (crash) via a crafted .ogg file.	2014-06-10	4.3	CVE-2014-3216
google -- chrome	net/spdy/spdy_write_queue.cc in the SPDY implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging incorrect queue maintenance.	2014-06-11	5.0	CVE-2014-3155
gordon_heydon -- secure_pages	The Secure Pages module 6.x-2.x before 6.x-2.0 for Drupal does not properly match URLs, which causes HTTP to be used instead of HTTPS and makes it easier for remote attackers to obtain sensitive	2014-06-09	5.0	CVE-2013-4595

	information via a crafted web page.			
ibm -- connections	Cross-site request forgery (CSRF) vulnerability in the Profiles component in IBM Connections through 3.0.1.1 CR3 allows remote authenticated users to hijack the authentication of arbitrary users for requests that trigger follow actions.	2014-06-08	6.0	CVE-2014-0929
ibm -- security_appscan_source	IBM Security AppScan Source 8.0 through 9.0, when the publish-assessment permission is not properly restricted for the configured database server, transmits cleartext assessment data, which allows remote attackers to obtain sensitive information by sniffing the network.	2014-06-08	4.3	CVE-2014-0936
ibm -- security_identity_manager	Cross-site request forgery (CSRF) vulnerability in IBM Tivoli Identity Manager (ITIM) 5.0 before 5.0.0.15 and 5.1 before 5.1.0.15 and IBM Security Identity Manager (ISIM) 6.0 before 6.0.0.2 allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences.	2014-06-08	6.0	CVE-2014-0961
ibm -- api_management	Unspecified vulnerability in IBM API Management 3.0.0.0, when basic authentication is used for APIs, allows remote attackers to bypass intended restrictions on topology access, and obtain sensitive information, via unknown vectors.	2014-06-08	4.3	CVE-2014-3036
ibm -- cics_transaction_server	IBM CICS Transaction Server 3.1, 3.2, 4.1, 4.2, and 5.1 on z/OS does not properly implement CEMT transactions, which allows remote authenticated users to cause a denial of service (storage overlay) by using a 3270 emulator to send an invalid 3270 data stream.	2014-06-10	4.0	CVE-2014-3042
ibm -- system_storage_virtualization_engine_ts7700	Unspecified vulnerability on the IBM System Storage Virtualization Engine TS7700 allows local users to gain privileges by leveraging the TSSC service-user role to enter a crafted SSH command.	2014-06-08	6.0	CVE-2014-3048
ibm -- aix	libodm.a in IBM AIX 6.1 and 7.1, and VIOS 2.2.x, allows local users to overwrite arbitrary files via a symlink attack on a temporary file. NOTE: this vulnerability exists because of an incomplete fix for	2014-06-08	6.9	CVE-2014-3977

	CVE-2012-2179.			
impresscms -- impresscms	Cross-site scripting (XSS) vulnerability in modules/system/admin.php in ImpressCMS 1.3.6.1 allows remote attackers to inject arbitrary web script or HTML via the query parameter in a listimg action.	2014-06-11	4.3	CVE-2014-4036
jasig -- phpcas	phpCAS before 1.3.2 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.	2014-06-06	5.8	CVE-2012-5583
jojocms -- jojo-cms	Cross-site scripting (XSS) vulnerability in plugins/jojo_core/forgot_password.php in Jojo before 1.2.2 allows remote attackers to inject arbitrary web script or HTML via the search parameter to forgot-password/.	2014-06-09	4.3	CVE-2013-3082
jzip -- jzip	Stack-based buffer overflow in Jzip 1.3 through 2.0.0.132900 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long file name in a zip archive.	2014-06-11	6.8	CVE-2010-5300
mambo-foundation -- mambo_cms	Mambo CMS 4.6.5 allows remote attackers to cause a denial of service (memory and bandwidth consumption) by uploading a crafted file.	2014-06-09	5.0	CVE-2013-2564
member_approval_plugin_project -- member_approval	Cross-site request forgery (CSRF) vulnerability in the Member Approval plugin 131109 for WordPress allows remote attackers to hijack the authentication of administrators for requests that change plugin settings to their default and disable registration approval via a request to wp-admin/options-general.php.	2014-06-11	6.8	CVE-2014-3850
microsoft -- windows_7	The Remote Desktop Protocol (RDP) implementation in Microsoft Windows 7 SP1, Windows 8, Windows 8.1, and Windows Server 2012 Gold and R2 does not properly encrypt sessions, which makes it easier for man-in-the-middle attackers to obtain sensitive information by sniffing the network or modify session content by sending	2014-06-11	5.1	CVE-2014-0296

	crafted RDP packets, aka "RDP MAC Vulnerability."			
microsoft -- internet_explorer	SChannel in Microsoft Internet Explorer 6 through 11 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which allows man-in-the-middle attackers to obtain sensitive information or modify TLS session data via a "triple handshake attack," aka "TLS Server Certificate Renegotiation Vulnerability."	2014-06-11	6.8	CVE-2014-1771
microsoft -- internet_explorer	Microsoft Internet Explorer 10 and 11 allows remote attackers to read local files on the client via a crafted web site, aka "Internet Explorer Information Disclosure Vulnerability."	2014-06-11	4.3	CVE-2014-1777
microsoft -- internet_explorer	Microsoft Internet Explorer 8 through 11 allows remote attackers to execute arbitrary web script with increased privileges via unspecified vectors, aka "Internet Explorer Elevation of Privilege Vulnerability," a different vulnerability than CVE-2014-2777.	2014-06-11	6.8	CVE-2014-1778
microsoft -- windows_7	The TCP implementation in Microsoft 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 allows remote attackers to cause a denial of service (non-paged pool memory consumption and system hang) via malformed data in the Options field of a TCP header, aka "TCP Denial of Service Vulnerability."	2014-06-11	5.0	CVE-2014-1811
microsoft -- xml_core_services	Microsoft XML Core Services (aka MSXML) 3.0 and 6.0 does not properly restrict the information transmitted by Internet Explorer during a download action, which allows remote attackers to discover (1) full pathnames on the client system and (2) local usernames embedded in these pathnames via a crafted web site, aka "MSXML Entity URI Vulnerability."	2014-06-11	4.3	CVE-2014-1816
microsoft -- lync_server	Cross-site scripting (XSS) vulnerability in the Web Components Server in Microsoft Lync Server 2010 and 2013 allows remote attackers to inject arbitrary	2014-06-11	4.3	CVE-2014-1823

	web script or HTML via a crafted URL containing a valid meeting ID, aka "Lync Server Content Sanitization Vulnerability."			
misery_project -- misery_6.x-2.0	The Misery module 6.x-2.x before 6.x-2.5 and 7.x-2.x before 7.x-2.2 for Drupal, when the "delay misery" configuration is set to a high value, allows remote attackers to cause a denial of service (process consumption) via multiple requests.	2014-06-09	4.3	CVE-2013-4599
mozilla -- firefox	Mozilla Firefox before 30.0 and Thunderbird through 24.6 on OS X do not ensure visibility of the cursor after interaction with a Flash object and a DIV element, which makes it easier for remote attackers to conduct clickjacking attacks via JavaScript code that produces a fake cursor image.	2014-06-11	5.0	CVE-2014-1539
mozilla -- firefox	Buffer overflow in the Speex resampler in the Web Audio subsystem in Mozilla Firefox before 30.0 allows remote attackers to execute arbitrary code via vectors related to a crafted AudioBuffer channel count and sample rate.	2014-06-11	6.8	CVE-2014-1542
qnap -- photo_station	QNAP Photo Station before firmware 4.0.3 build0912 allows remote attackers to list OS user accounts via a request to photo/p/api/list.php.	2014-06-09	5.0	CVE-2013-5760
rik_de_boer -- revisioning	The Revisioning module 7.x-1.x before 7.x-1.6 for Drupal does not properly check node access permissions for content marked unpublished by the Scheduled module, which allows remote authenticated users to obtain sensitive information via unspecified vectors.	2014-06-09	4.0	CVE-2013-4597
sap -- project_system	The (1) Structures and (2) Project-Oriented Procurement components in SAP Project System has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4004
sap -- brazil	SAP Brazil add-on has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4005
sap --	The SAP Trader's and Scheduler's Workbench (TSW)	2014-06-09	5.0	CVE-2014-4006

oil_industry_solution_traders_and_schedulers_workbench	for SAP Oil & Gas has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.			
sap -- upgrade_tools	The SAP Upgrade tools for ABAP has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4007
sap -- web_services_tool	SAP Web Services Tool (CA-WUI-WST) has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4008
sap -- computing_center_management_system_monitoring	SAP CCMS Monitoring (BC-CCM-MON) has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4009
sap -- transaction_data_pool	SAP Transaction Data Pool has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4010
sap -- capacity_leveling	SAP Capacity Leveling has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4011
sap -- open_hub_service	SAP Open Hub Service has hardcoded credentials, which makes it easier for remote attackers to obtain access via unspecified vectors.	2014-06-09	5.0	CVE-2014-4012

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
cisofy -- lynis	include/tests_webservers in Lynis before 1.5.5 on	2014-06-08	3.3	CVE-2014-3982

	AIX allows local users to overwrite arbitrary files via a symlink attack on a /tmp/lynis.##### file.			
cisofy -- lynis	include/tests_webservers in Lynis before 1.5.5 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/lynis.*.unsorted file with an easily determined name.	2014-06-08	3.3	CVE-2014-3986
fedoraproject -- sssd	The System Security Services Daemon (SSSD) 1.11.6 does not properly identify group membership when a non-POSIX group is in a group membership chain, which allows local users to bypass access restrictions via unspecified vectors.	2014-06-11	3.3	CVE-2014-0249
freebsd -- freebsd	The ktrace utility in the FreeBSD kernel 8.4 before p11, 9.1 before p14, 9.2 before p7, and 9.3-BETA1 before p1 uses an incorrect page fault kernel trace entry size, which allows local users to obtain sensitive information from kernel memory via a kernel process trace.	2014-06-10	2.1	CVE-2014-3873
ibm -- spss_modeler	IBM SPSS Modeler 16.0 before 16.0.0.1 on UNIX does not properly drop group privileges, which allows local users to bypass intended file-access restrictions by leveraging (1) gid 0 or (2) root's group memberships.	2014-06-08	3.6	CVE-2014-3038
livezilla -- livezilla	LiveZilla before 5.1.1.0 stores the admin Base64 encoded username and password in a 1click file, which allows local users to obtain access by reading the file.	2014-06-09	2.1	CVE-2013-6223
mambo-foundation -- mambo_cms	Mambo CMS 4.6.5 stores the MySQL database password in cleartext in the document root, which allows local users to obtain sensitive information via unspecified vectors.	2014-06-09	2.1	CVE-2013-2562
mambo-foundation -- mambo_cms	Mambo CMS 4.6.5 uses world-readable permissions on configuration.php, which allows local users to obtain the admin password hash by reading the file.	2014-06-09	2.1	CVE-2013-2563
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in Special:PasswordReset in MediaWiki before 1.19.16, 1.21.x before 1.21.10, and 1.22.x before 1.22.7, when wgRawHtml is enabled, allows remote attackers to	2014-06-06	2.6	CVE-2014-3966

	inject arbitrary web script or HTML via an invalid username.			
php -- php	acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.	2014-06-08	3.3	CVE-2014-3981
pulseaudio -- pulseaudio	The pa_rtp_recv function in modules/rtp/rtp.c in the module-rtp-recv module in PulseAudio 5.0 and earlier allows remote attackers to cause a denial of service (assertion failure and abort) via an empty UDP packet.	2014-06-11	2.9	CVE-2014-3970
cisofy -- lynis	include/tests_webservers in Lynis before 1.5.5 on AIX allows local users to overwrite arbitrary files via a symlink attack on a /tmp/lynis.##### file.	2014-06-08	3.3	CVE-2014-3982
cisofy -- lynis	include/tests_webservers in Lynis before 1.5.5 allows local users to overwrite arbitrary files via a symlink attack on a /tmp/lynis.*.unsorted file with an easily determined name.	2014-06-08	3.3	CVE-2014-3986
fedoraproject -- sssd	The System Security Services Daemon (SSSD) 1.11.6 does not properly identify group membership when a non-POSIX group is in a group membership chain, which allows local users to bypass access restrictions via unspecified vectors.	2014-06-11	3.3	CVE-2014-0249
freebsd -- freebsd	The ktrace utility in the FreeBSD kernel 8.4 before p11, 9.1 before p14, 9.2 before p7, and 9.3-BETA1 before p1 uses an incorrect page fault kernel trace entry size, which allows local users to obtain sensitive information from kernel memory via a kernel process trace.	2014-06-10	2.1	CVE-2014-3873
ibm -- spss_modeler	IBM SPSS Modeler 16.0 before 16.0.0.1 on UNIX does not properly drop group privileges, which allows local users to bypass intended file-access restrictions by leveraging (1) gid 0 or (2) root's group memberships.	2014-06-08	3.6	CVE-2014-3038
livezilla -- livezilla	LiveZilla before 5.1.1.0 stores the admin Base64 encoded username and password in a 1click file, which allows local users to obtain access by reading	2014-06-09	2.1	CVE-2013-6223

	the file.			
mambo-foundation -- mambo_cms	Mambo CMS 4.6.5 stores the MySQL database password in cleartext in the document root, which allows local users to obtain sensitive information via unspecified vectors.	2014-06-09	2.1	CVE-2013-2562
mambo-foundation -- mambo_cms	Mambo CMS 4.6.5 uses world-readable permissions on configuration.php, which allows local users to obtain the admin password hash by reading the file.	2014-06-09	2.1	CVE-2013-2563
mediawiki -- mediawiki	Cross-site scripting (XSS) vulnerability in Special:PasswordReset in MediaWiki before 1.19.16, 1.21.x before 1.21.10, and 1.22.x before 1.22.7, when wgRawHtml is enabled, allows remote attackers to inject arbitrary web script or HTML via an invalid username.	2014-06-06	2.6	CVE-2014-3966
php -- php	acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.	2014-06-08	3.3	CVE-2014-3981
pulseaudio -- pulseaudio	The pa_rtp_recv function in modules/rtp/rtp.c in the module-rtp-recv module in PulseAudio 5.0 and earlier allows remote attackers to cause a denial of service (assertion failure and abort) via an empty UDP packet.	2014-06-11	2.9	CVE-2014-3970

- 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).