Vulnerability Summary for the Week of February 13, 2017

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**
adobe -- campaign	Adobe Campaign versions 16.4 Build 8724 and earlier have a code injection vulnerability.	2017-02-15	7.5	CVE-2017-2968 CONFIRM (link is external) CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable heap overflow vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2973 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2982 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the h264 decoder routine. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2984 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and	2017-02-15	10.0	CVE-2017-2985

	earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code execution.			CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the Flash Video (FLV) codec. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2986 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable integer overflow vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2987 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability when performing garbage collection. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2988 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 decompression routine. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2990 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 codec (related to decompression). Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2991 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability when parsing an MP4 header. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2992 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability related to event handlers. Successful exploitation could lead to arbitrary	2017-02-15	10.0	CVE-2017-2993 CONFIRM (link is external)

	code execution.			
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in Primetime SDK. Successful exploitation could lead to arbitrary code execution.	2017-02-15	10.0	CVE-2017-2996 CONFIRM (link is external)
advantech -- susiaccess	An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. The admin password is stored in the system and is encrypted with a static key hard-coded in the program. Attackers could reverse the admin account password for use.	2017-02-13	7.2	CVE-2016-9353 BID (link is external) MISC
advantech -- webaccess	An issue was discovered in Advantech WebAccess Version 8.1. To be able to exploit the SQL injection vulnerability, an attacker must supply malformed input to the WebAccess software. Successful attack could result in administrative access to the application and its data files.	2017-02-13	7.5	CVE-2017-5154 BID (link is external) MISC
binom3 -- universal_multifunctional_electric_power_quality_meter_firmware	An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Lack of authentication for remote service gives access to application set up and configuration.	2017-02-13	10.0	CVE-2017-5162 BID (link is external) MISC
binom3 -- universal_multifunctional_electric_power_quality_meter_firmware	An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Users do not have any option to change their own passwords.	2017-02-13	7.5	CVE-2017-5167 BID (link is external) MISC
dotcms -- dotcms	An issue was discovered in dotCMS through 3.6.1. The findChildrenByFilter() function which is called by the web accessible path /categoriesServlet performs string interpolation and direct SQL query execution. SQL quote escaping and a keyword blacklist were implemented in a new class, SQLUtil (main/java/com/dotmarketing/common/util/SQLUtil.java), as part of the remediation of CVE-2016-8902; however, these can be overcome in the case of the q and inode parameters to the	2017-02-17	7.5	CVE-2017-5344 MISC (link is external) MISC MISC (link is external)

	/categoriesServlet path. Overcoming these controls permits a number of blind boolean SQL injection vectors in either parameter. The /categoriesServlet web path can be accessed remotely and without authentication in a default dotCMS deployment.			
exponentcms -- exponent_cms	install/index.php in Exponent CMS 2.3.9 allows remote attackers to execute arbitrary commands via shell metacharacters in the sc array parameter.	2017-02-13	7.5	CVE-2016-7565 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
freebsd -- freebsd	The Linux compatibility layer in the kernel in FreeBSD 9.3, 10.1, and 10.2 allows local users to read portions of kernel memory and potentially gain privilege via unspecified vectors, related to "handling of Linux futex robust lists."	2017-02-15	7.2	CVE-2016-1880 SECTRACK (link is external) FREEBSD
freebsd -- freebsd	The kernel in FreeBSD 9.3, 10.1, and 10.2 allows local users to cause a denial of service (crash) or potentially gain privilege via a crafted Linux compatibility layer setgroups system call.	2017-02-15	7.2	CVE-2016-1881 SECTRACK (link is external) FREEBSD
freebsd -- freebsd	The issetugid system call in the Linux compatibility layer in FreeBSD 9.3, 10.1, and 10.2 allows local users to gain privilege via unspecified vectors.	2017-02-15	7.2	CVE-2016-1883 SECTRACK (link is external) FREEBSD
freebsd -- freebsd	Integer overflow in the bhyve hypervisor in FreeBSD 10.1, 10.2, 10.3, and 11.0 when configured with a large amount of guest memory, allows local users to gain privilege via a crafted device descriptor.	2017-02-15	7.2	CVE-2016-1889 SECTRACK (link is external) FREEBSD
honeywell -- xl_web_ii_controller	An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. A user without authenticating can make a directory traversal attack by accessing a specific URL.	2017-02-13	7.5	CVE-2017-5143 BID (link is external) MISC
ibm -- integration_bus	IBM Integration Bus 9.0 and 10.0 and WebSphere Message Broker SOAP FLOWS is vulnerable to a	2017-02-15	8.5	CVE-2016-9706 CONFIRM (link is external)

	denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume all available memory resources. IBM Reference #: 1997918.			
ibm -- vios	IBM AIX 5.3, 6.1, 7.1, and 7.2 contains an unspecified vulnerability that would allow a locally authenticated user to obtain root level privileges. IBM APARs: IV88658, IV87981, IV88419, IV87640, IV88053.	2017-02-15	7.2	CVE-2016-6079 CONFIRM (link is external) BID (link is external)
ibm -- vios	IBM AIX 6.1, 7.1, and 7.2 could allow a local user to gain root privileges using a specially crafted command within the bellmail client. IBM APARs: IV91006, IV91007, IV91008, IV91010, IV91011.	2017-02-15	7.2	CVE-2016-8972 CONFIRM (link is external) BID (link is external)
lynxspring -- jenesys_bas_bridge	An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application uses a hard-coded username with no password allowing an attacker into the system without authentication.	2017-02-13	7.5	CVE-2016-8361 BID (link is external) MISC
moxa -- dacenter	An issue was discovered in Moxa DACenter Versions 1.4 and older. A specially crafted project file may cause the program to crash because of Uncontrolled Resource Consumption.	2017-02-13	7.1	CVE-2016-9354 BID (link is external) MISC
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Administration	2017-02-13	7.5	CVE-2016-9361 BID (link is external) MISC

	passwords can be retried without authenticating.			
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Buffer overflow vulnerability may allow an unauthenticated attacker to remotely execute arbitrary code.	2017-02-13	7.5	CVE-2016-9363 BID (link is external) MISC
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. The amount of resources requested by a malicious actor is not restricted, leading to a denial-of-service caused by resource exhaustion.	2017-02-13	7.8	CVE-2016-9367 BID (link is external) MISC
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to	2017-02-13	10.0	CVE-2016-9369 BID (link is external) MISC

	3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Firmware can be updated over the network without authentication, which may allow remote code execution.			
moxa -- softcms	An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. Moxa SoftCMS Webserver does not properly validate input. An attacker could provide unexpected values and cause the program to crash or excessive consumption of resources could result in a denial-of-service condition.	2017-02-13	7.8	CVE-2016-9332 BID (link is external) MISC
nagios -- nagios	Nagios 4.2.4 and earlier allows local users to gain root privileges via a hard link attack on the Nagios init script file, related to CVE-2016-8641.	2017-02-15	7.2	CVE-2016-10089 MLIST (link is external) BID (link is external)
schneider-electric -- powerlogic_pm8ecc_firmware	An issue was discovered in Schneider Electric PowerLogic PM8ECC device 2.651 and older. Undocumented hard-coded credentials allow access to the device.	2017-02-13	7.5	CVE-2016-5818 BID (link is external) MISC
videoinsight -- web_client	An issue was discovered in VideoInsight Web Client Version 6.3.5.11 and previous versions. A SQL Injection vulnerability has been identified, which may allow remote code execution.	2017-02-13	7.5	CVE-2017-5151 BID (link is external) MISC
vim -- vim	vim before patch 8.0.0322 does not properly validate values for tree length when handling a spell file, which may result in an integer overflow at a memory allocation site and a resultant buffer overflow.	2017-02-10	7.5	CVE-2017-5953 CONFIRM (link is external) CONFIRM (link is external)

wireshark -- wireshark	In Wireshark 2.2.4 and earlier, a crafted or malformed STANAG 4607 capture file will cause an infinite loop and memory exhaustion. If the packet size field in a packet header is null, the offset to read from will not advance, causing continuous attempts to read the same zero length packet. This will quickly exhaust all system memory.	2017-02-17	7.8	CVE-2017-6014 CONFIRM

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
adcon_telemetry -- a850_telemetry_gateway_base_station_firmware	An issue was discovered in Adcon Telemetry A850 Telemetry Gateway Base Station. The Web Interface does not neutralize or incorrectly neutralizes user-controllable input before it is placed in the output; this could allow for cross-site scripting.	2017-02-13	4.3	CVE-2016-2274 BID (link is external) MISC
adobe -- campaign	Adobe Campaign versions 16.4 Build 8724 and earlier have a cross-site scripting (XSS) vulnerability.	2017-02-15	4.3	CVE-2017-2969 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2974 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2975 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to	2017-02-15	5.0	CVE-2017-2976 CONFIRM (link is external)

	arbitrary code execution.			
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2977 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2978 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2979 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2980 CONFIRM (link is external)
adobe -- digital_editions	Adobe Digital Editions versions 4.5.3 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution.	2017-02-15	5.0	CVE-2017-2981 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in Primetime SDK event dispatch. Successful exploitation could lead to arbitrary code execution.	2017-02-15	6.8	CVE-2017-2994 CONFIRM (link is external)
adobe -- flash_player	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable type confusion vulnerability related to the MessageChannel class. Successful exploitation could lead to arbitrary code execution.	2017-02-15	6.8	CVE-2017-2995 CONFIRM (link is external)
advantech -- susiaccess	An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. An attacker could traverse the file system and extract files that can result in information disclosure.	2017-02-13	5.0	CVE-2016-9349 BID (link is external) MISC
advantech -- susiaccess	An issue was discovered in Advantech SUISAccess Server Version 3.0 and prior. The directory traversal/file upload error allows an attacker to upload and unpack a zip file.	2017-02-13	6.0	CVE-2016-9351 BID (link is external) MISC

advantech -- webaccess	An issue was discovered in Advantech WebAccess Version 8.1. By accessing a specific uniform resource locator (URL) on the web server, a malicious user is able to access pages unrestricted (AUTHENTICATION BYPASS).	2017-02-13	6.4	CVE-2017-5152 BID (link is external) MISC
artifex -- mupdf	The pdf_to_num function in pdf-object.c in MuPDF before 1.10 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted file.	2017-02-15	4.3	CVE-2016-8674 CONFIRM (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
artifex -- mupdf	Heap-based buffer overflow in the fz_subsample_pixmap function in fitz/pixmap.c in MuPDF 1.10a allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted image.	2017-02-15	4.3	CVE-2017-5896 CONFIRM (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
autotrace_project -- autotrace	Heap-based buffer overflow in the pstoedit_suffix_table_init function in output-pstoedit.c in AutoTrace 0.31.1 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted bmp image file.	2017-02-15	4.3	CVE-2016-7392 MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
binom3 -- universal_multifunctional_electric_power_quality_meter_firmware	An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. Input sent from a malicious client is not properly verified by the server. An attacker can execute arbitrary script code in another user's browser session (CROSS-SITE SCRIPTING).	2017-02-13	4.3	CVE-2017-5164 BID (link is external) MISC

binom3 -- universal_multifunctional_electric_power_quality_meter_firmware	An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. There is no CSRF Token generated per page and/or per (sensitive) function. Successful exploitation of this vulnerability can allow silent execution of unauthorized actions on the device such as configuration parameter changes, and saving modified configuration.	2017-02-13	6.8	CVE-2017-5165 BID (link is external) MISC
binom3 -- universal_multifunctional_electric_power_quality_meter_firmware	An issue was discovered in BINOM3 Universal Multifunctional Electric Power Quality Meter. An INFORMATION EXPOSURE flaw can be used to gain privileged access to the device.	2017-02-13	5.0	CVE-2017-5166 BID (link is external) MISC
bubblewrap_project -- bubblewrap	Bubblewrap before 0.1.3 sets the PR_SET_DUMPABLE flag, which might allow local users to gain privileges by attaching to the process, as demonstrated by sending commands to a PrivSep socket.	2017-02-13	6.9	CVE-2016-8659 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
fatek -- automation_pm_designer	An issue was discovered in Fatek Automation PM Designer V3 Version 2.1.2.2, and Automation FV Designer Version 1.2.8.0. Sending additional valid packets could allow the attacker to cause a crash or to execute arbitrary code, because of Improper Restriction of Operations within the Bounds of a Memory Buffer.	2017-02-13	6.8	CVE-2016-5796 BID (link is external) MISC
fatek -- automation_pm_designer	An issue was discovered in Fatek Automation PM Designer V3 Version 2.1.2.2, and Automation FV Designer Version 1.2.8.0. By sending additional valid packets, an attacker could trigger a stack-based buffer overflow and cause a crash. Also, a malicious attacker can trigger a remote buffer overflow on the Fatek Communication Server.	2017-02-13	5.0	CVE-2016-5798 BID (link is external) MISC
fedoraproject -- fedora	slock allows attackers to bypass the screen lock via vectors involving an invalid password hash, which triggers a NULL pointer dereference and crash.	2017-02-15	5.0	CVE-2016-6866 CONFIRM MISC (link is external) MLIST (link is external)

				MLIST (link is external) BID (link is external) FEDORA FEDORA
fedoraproject -- fedora	regex.c in GNU ed before 1.14.1 allows attackers to cause a denial of service (crash) via a malformed command, which triggers an invalid free.	2017-02-16	5.0	CVE-2017-5357 MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) FEDORA MLIST
freebsd -- freebsd	The telnetd service in FreeBSD 9.3, 10.1, 10.2, 10.3, and 11.0 allows remote attackers to inject arguments to login and bypass authentication via vectors involving a "sequence of memory allocation failures."	2017-02-15	5.0	CVE-2016-1888 SECTRACK (link is external) FREEBSD
gnu -- glibc	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.	2017-02-16	5.0	CVE-2016-5417 MLIST (link is external) BID (link is external) CONFIRM CONFIRM MLIST
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5006 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5007 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5008 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2017-02-17	6.8	CVE-2017-5009 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5010 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5011 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2017-02-17	6.8	CVE-2017-5012 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5013 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for	2017-02-17	6.8	CVE-2017-5014 BID (link is external) CONFIRM (link is external)

	Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.			CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.	2017-02-17	4.3	CVE-2017-5015 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5016 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	2017-02-17	6.8	CVE-2017-5019 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5020 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5022 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null	2017-02-17	4.3	CVE-2017-5023 BID (link is external) CONFIRM (link is external) CONFIRM (link

	dereference via a crafted HTML page.			is external)
google -- chrome	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.	2017-02-17	4.3	CVE-2017-5025 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5026 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- chrome	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.	2017-02-17	4.3	CVE-2017-5027 CONFIRM (link is external) CONFIRM (link is external)
gosa_project -- gosa_plugin	Cross-site scripting (XSS) vulnerability in the displayLogin function in html/index.php in GOsa allows remote attackers to inject arbitrary web script or HTML via the username.	2017-02-13	4.3	CVE-2014-9760 MLIST (link is external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	The ReadSCTImage function in coders/sct.c in GraphicsMagick 1.3.25 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted SCT header.	2017-02-15	5.0	CVE-2016-8682 CONFIRM (link is external) SUSE DEBIAN MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
graphicsmagick -- graphicsmagick	The ReadPCXImage function in coders/pcx.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."	2017-02-15	6.8	CVE-2016-8683 CONFIRM (link is external) SUSE DEBIAN MLIST (link is external) BID (link is external)

				MISC CONFIRM (link is external)
graphicsmagick -- graphicsmagick	The MagickMalloc function in magick/memory.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."	2017-02-15	6.8	CVE-2016-8684 CONFIRM (link is external) SUSE DEBIAN MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
honeywell -- xl_web_ii_controller	An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. Any user is able to disclose a password by accessing a specific URL, because of Plaintext Storage of a Password.	2017-02-13	5.0	CVE-2017-5139 BID (link is external) MISC
honeywell -- xl_web_ii_controller	An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. Password is stored in clear text.	2017-02-13	5.0	CVE-2017-5140 BID (link is external) MISC
honeywell -- xl_web_ii_controller	An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. An attacker can establish a new user session, without invalidating any existing session identifier, which gives the opportunity to steal authenticated sessions (SESSION FIXATION).	2017-02-13	6.5	CVE-2017-5141 BID (link is external) MISC
honeywell -- xl_web_ii_controller	An issue was discovered in Honeywell XL Web II controller XL1000C500 XLWebExe-2-01-00 and prior, and XLWeb 500 XLWebExe-1-02-08 and prior. A user with low privileges is able to open and change the parameters by accessing a specific URL because of Improper Privilege Management.	2017-02-13	6.5	CVE-2017-5142 BID (link is external) MISC
ibm -- aix	IBM AIX 7.1 and 7.2 allows a local user to open a file with a specially crafted argument that would crash the system. IBM APARs: IV91488, IV91487, IV91456,	2017-02-15	4.9	CVE-2016-8944 CONFIRM (link is external) BID (link is external)

	IV90234.			
ibm -- cognos_disclosure_management	IBM Cognos Disclosure Management 10.2 could allow a malicious attacker to execute commands as a lower privileged user that opens a malicious document. IBM Reference #: 1991584.	2017-02-15	6.8	CVE-2016-6077 CONFIRM (link is external) BID (link is external)
ibm -- integration_bus	IBM WebSphere Message Broker 9.0 and 10.0 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM Reference #: 1997906.	2017-02-15	4.3	CVE-2016-9010 CONFIRM (link is external)
ibm -- rational_requirements_composer	An undisclosed vulnerability in IBM Rational DOORS Next Generation 4.0, 5.0, and 6.0 could allow a JazzGuest user to see project names. IBM Reference #: 1995547.	2017-02-15	4.0	CVE-2016-6060 CONFIRM (link is external)
kabona_ab -- webdatorcentral	An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. The web server URL inputs are not sanitized correctly, which may allow cross-site scripting vulnerabilities.	2017-02-13	4.3	CVE-2016-8356 BID (link is external) MISC
kabona_ab -- webdatorcentral	An issue was discovered in Kabona AB WebDatorCentral (WDC) application prior to Version 3.4.0. This non-validated redirect/non-validated forward (OPEN REDIRECT) allows chaining with authenticated vulnerabilities.	2017-02-13	5.8	CVE-2016-8376 BID (link is external) MISC
libav -- libav	Heap-based buffer overflow in the ff_audio_resample function in resample.c in libav before 11.4 allows remote attackers to cause a denial of service (crash) via vectors related to buffer resizing.	2017-02-15	4.3	CVE-2016-6832 MLIST (link is external) MLIST (link is external) MISC CONFIRM CONFIRM
libav -- libav	Stack-based buffer overflow in the aac_sync function in aac_parser.c in Libav before 11.5 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.	2017-02-15	4.3	CVE-2016-7393 MLIST (link is external) BID (link is external) MISC CONFIRM

libav -- libav	The ff_put_pixels8_xy2_mmx function in rnd_template.c in Libav 11.7 allows remote attackers to cause a denial of service (invalid memory access and crash) via a crafted mp3 file. NOTE: this issue was originally reported as involving a NULL pointer dereference.	2017-02-15	4.3	CVE-2016-7477 MLIST (link is external) BID (link is external) MISC
libav -- libav	The sbr_make_f_master function in aacsbr.c in Libav 11.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted mp3 file.	2017-02-15	4.3	CVE-2016-7499 MLIST (link is external) BID (link is external) MISC CONFIRM
libav -- libav	The get_vlc2 function in get_bits.h in Libav before 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file, possibly related to startcode sequences during m4v detection.	2017-02-15	4.3	CVE-2016-8675 MLIST (link is external) BID (link is external) MISC CONFIRM (link is external)
libav -- libav	The get_vlc2 function in get_bits.h in Libav 11.9 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted mp3 file. NOTE: this issue exists due to an incomplete fix for CVE-2016-8675.	2017-02-15	4.3	CVE-2016-8676 MLIST (link is external) MLIST (link is external) BID (link is external) MISC MISC
libdwarf_project -- libdwarf	libdwarf 20151114 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a debug_abbrev section marked NOBITS in an ELF file.	2017-02-13	4.3	CVE-2015-8750 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external)
libming -- libming	The _iprintf function in outputtxt.c in the listswf tool in libming 0.4.7 allows remote attackers to cause a denial of service (buffer over-read) via a crafted SWF file.	2017-02-16	4.3	CVE-2016-9827 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
libming -- libming	The dumpBuffer function in read.c in the listswf tool in libming 0.4.7 allows remote attackers to cause a	2017-02-16	4.3	CVE-2016-9828 MLIST (link is external)

	denial of service (NULL pointer dereference) via a crafted SWF file.			MLIST (link is external) BID (link is external) MISC
libming -- libming	Heap-based buffer overflow in the parseSWF_DEFINEFONT function in parser.c in the listswf tool in libming 0.4.7 allows remote attackers to have unspecified impact via a crafted SWF file.	2017-02-16	6.8	CVE-2016-9829 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
libming -- libming	Heap-based buffer overflow in the parseSWF_RGBA function in parser.c in the listswf tool in libming 0.4.7 allows remote attackers to have unspecified impact via a crafted SWF file.	2017-02-16	6.8	CVE-2016-9831 MLIST (link is external) MLIST (link is external) BID (link is external) MISC
linux -- linux_kernel	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.	2017-02-14	5.0	CVE-2017-5970 CONFIRM MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM
lynxspring -- jenesys_bas_bridge	An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. A user with read-only access can send commands to the software and the application will accept those commands. This would allow an attacker with read-only access to make changes within the application.	2017-02-13	5.5	CVE-2016-8357 BID (link is external) MISC
lynxspring -- jenesys_bas_bridge	An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application does not sufficiently verify if a request was intentionally provided by the user who submitted the request (CROSS-SITE REQUEST FORGERY).	2017-02-13	6.8	CVE-2016-8369 BID (link is external) MISC
lynxspring -- jenesys_bas_bridge	An issue was discovered in Lynxspring JENEsys BAS Bridge versions 1.1.8 and older. The application's database lacks sufficient safeguards for protecting credentials.	2017-02-13	5.0	CVE-2016-8378 BID (link is external) MISC

mariadb -- mariadb	Crash in libmysqlclient.so in Oracle MySQL before 5.6.21 and 5.7.x before 5.7.5 and MariaDB through 5.5.54, 10.0.x through 10.0.29, 10.1.x through 10.1.21, and 10.2.x through 10.2.3.	2017-02-11	5.0	CVE-2017-3302 MISC (link is external)
moxa -- dacenter	An issue was discovered in Moxa DACenter Versions 1.4 and older. The application may suffer from an unquoted search path issue.	2017-02-13	4.6	CVE-2016-9356 BID (link is external) MISC
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. Requests are not verified to be intentionally submitted by the proper user (CROSS-SITE REQUEST FORGERY).	2017-02-13	6.8	CVE-2016-9365 BID (link is external) MISC
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. An attacker can freely use brute force to determine parameters needed to bypass authentication.	2017-02-13	5.0	CVE-2016-9366 BID (link is external) MISC

moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. User-controlled input is not neutralized before being output to web page (CROSS-SITE SCRIPTING).	2017-02-13	4.3	CVE-2016-9371 BID (link is external) MISC
moxa -- softcms	An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. A specially crafted URL request sent to the SoftCMS ASP Webserver can cause a double free condition on the server allowing an attacker to modify memory locations and possibly cause a denial of service or the execution of arbitrary code.	2017-02-13	6.8	CVE-2016-8360 BID (link is external) MISC
moxa -- softcms	An issue was discovered in Moxa SoftCMS versions prior to Version 1.6. The SoftCMS Application does not properly sanitize input that may allow a remote attacker access to SoftCMS with administrator's privilege through specially crafted input (SQL INJECTION).	2017-02-13	6.5	CVE-2016-9333 BID (link is external) MISC
nitro_software -- nitro_pro	A remote out of bound write / memory corruption vulnerability exists in the PDF parsing functionality of Nitro Pro 10. A specially crafted PDF file can cause a vulnerability resulting in potential memory corruption. An attacker can send the victim a specific PDF file to trigger this vulnerability.	2017-02-10	6.8	CVE-2016-8709 MISC (link is external)
nitro_software -- nitro_pro	A potential remote code execution vulnerability exists in the PDF parsing functionality of Nitro Pro 10. A specially crafted PDF file can cause a vulnerability resulting in potential code execution. An attacker can send the victim a specific PDF file to	2017-02-10	6.8	CVE-2016-8711 MISC (link is external)

	trigger this vulnerability.			
omnimetrix -- omniview	An issue was discovered in OmniMetrix OmniView, Version 1.2. The OmniView web application transmits credentials with the HTTP protocol, which could be sniffed by an attacker that may result in the compromise of account credentials.	2017-02-13	5.0	CVE-2016-5786 BID (link is external) MISC
omnimetrix -- omniview	An issue was discovered in OmniMetrix OmniView, Version 1.2. Insufficient password requirements for the OmniView web application may allow an attacker to gain access by brute forcing account passwords.	2017-02-13	5.0	CVE-2016-5801 BID (link is external) MISC
opensuse_project -- leap	Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename.	2017-02-15	5.0	CVE-2016-8687 SUSE MLIST (link is external) BID (link is external) MISC CONFIRM (link is external) MISC (link is external) GENTOO
opensuse_project -- leap	The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read-ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2) bid_entry function in libarchive/archive_read_support_format_mtree.c.	2017-02-15	4.3	CVE-2016-8688 SUSE MLIST (link is external) BID (link is external) MISC MISC MISC MISC MISC CONFIRM (link is external) CONFIRM (link is external) GENTOO
opensuse_project -- leap	The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive.	2017-02-15	5.0	CVE-2016-8689 SUSE MLIST (link is external) BID (link is external) MISC CONFIRM (link

				is external) CONFIRM (link is external) GENTOO
otrs -- otrs	Cross-site scripting (XSS) vulnerability in Open Ticket Request System (OTRS) 3.3.x before 3.3.16, 4.0.x before 4.0.19, and 5.0.x before 5.0.14 allows remote attackers to inject arbitrary web script or HTML via a crafted attachment.	2017-02-16	4.3	CVE-2016-9139 BID (link is external) CONFIRM (link is external)
python -- openpyxl	Openpyxl 2.4.1 resolves external entities by default, which allows remote attackers to conduct XXE attacks via a crafted .xlsx document.	2017-02-15	5.8	CVE-2017-5992 CONFIRM (link is external) CONFIRM CONFIRM CONFIRM
samsung -- samsung_mobile	Samsung devices with Android KK(4.4), L(5.0/5.1), or M(6.0) allow attackers to cause a denial of service (system crash) via a crafted system call to TvoutService_C.	2017-02-13	5.0	CVE-2016-4547 CONFIRM (link is external) MLIST (link is external)
schneider_electric -- homelynk_controller_lss100100_firmware	An issue was discovered in Schneider Electric homeLYnk Controller, LSS100100, all versions prior to V1.5.0. The homeLYnk controller is susceptible to a cross-site scripting attack. User inputs can be manipulated to cause execution of JavaScript code.	2017-02-13	4.3	CVE-2017-5157 BID (link is external) MISC
visonic -- powerlink2_firmware	An issue was discovered in Visonic PowerLink2, all versions prior to October 2016 firmware release. User controlled input is not neutralized prior to being placed in web page output (CROSS-SITE SCRIPTING).	2017-02-13	4.3	CVE-2016-5811 BID (link is external) MISC
wordpress -- mail_plugin	An issue was discovered in the WP Mail plugin before 1.2 for WordPress. The replyto parameter when composing a mail allows for a reflected XSS. This would allow you to execute JavaScript in the context of the user receiving the mail.	2017-02-10	4.3	CVE-2017-5942 MISC (link is external)
wso2 -- carbon	Directory traversal vulnerability in the LogViewer Admin Service in WSO2 Carbon 4.4.5 allows remote authenticated administrators to read arbitrary files via a .. (dot dot) in the logFile parameter to downloadgz-ajaxprocessor.jsp.	2017-02-16	4.0	CVE-2016-4314 MISC MISC (link is external) BUGTRAQ (link is external) BID (link is external)

				CONFIRM (link is external) EXPLOIT-DB (link is external)
wso2 -- carbon	Multiple cross-site scripting (XSS) vulnerabilities in WSO2 Carbon 4.4.5 allow remote attackers to inject arbitrary web script or HTML via the (1) setName parameter to identity-mgt/challenges-mgt.jsp; the (2) webappType or (3) httpPort parameter to webapp-list/webapp_info.jsp; the (4) dsName or (5) description parameter to ndatasource/newdatasource.jsp; the (6) phase parameter to viewflows/handlers.jsp; or the (7) url parameter to ndatasource/validateconnection-ajaxprocessor.jsp.	2017-02-16	4.3	CVE-2016-4316 MISC MISC (link is external) BUGTRAQ (link is external) BID (link is external) EXPLOIT-DB (link is external)
wso2 -- enablement_server_for_java	Cross-site scripting (XSS) vulnerability in WSO2 SOA Enablement Server for Java/6.6 build SSJ-6.6-20090827-1616 and earlier allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO.	2017-02-16	4.3	CVE-2016-4327 MISC (link is external) BUGTRAQ (link is external) BID (link is external)

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
bigtreecms -- bigtree_cms	An issue was discovered in BigTree CMS before 4.2.15. The vulnerability exists due to insufficient filtration of user-supplied data in the "id" HTTP GET parameter passed to the "core/admin/adjax/dashboard/check-module-integrity.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-02-14	3.5	CVE-2016-10223 CONFIRM (link is external) CONFIRM (link is external)

ibm -- rational_collaborative_lifecycle_management	IBM Jazz Foundation is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1998515.	2017-02-15	3.5	CVE-2016-8968 CONFIRM (link is external)
ibm -- websphere_application_server	IBM WebSphere Application Server 7.0, 8.0, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1997743	2017-02-13	3.5	CVE-2017-1121 CONFIRM (link is external)
linux -- linux_kernel	The time subsystem in the Linux kernel through 4.9.9, when CONFIG_TIMER_STATS is enabled, allows local users to discover real PID values (as distinguished from PID values inside a PID namespace) by reading the /proc/timer_list file, related to the print_timer function in kernel/time/timer_list.c and the __timer_stats_timer_set_start_info function in kernel/time/timer.c.	2017-02-14	2.1	CVE-2017-5967 CONFIRM MISC
mcafee -- epolicy_orchestrator	Cross-site scripting (XSS) vulnerability in the Web user interface (UI) in Intel Security ePO 5.1.3, 5.1.2, 5.1.1, and 5.1.0 allows authenticated users to inject malicious Java scripts via bypassing input validation.	2017-02-13	3.5	CVE-2017-3902 CONFIRM (link is external)
moxa -- nport_5100_series_firmware	An issue was discovered in Moxa NPort 5110 versions prior to 2.6, NPort 5130/5150 Series versions prior to 3.6, NPort 5200 Series versions prior to 2.8, NPort 5400 Series versions prior to 3.11, NPort 5600 Series versions prior to 3.7, NPort 5100A Series & NPort P5150A versions prior to 1.3, NPort 5200A Series versions prior to 1.3, NPort 5150AI-M12 Series versions prior to 1.2, NPort 5250AI-M12 Series versions prior to 1.2, NPort 5450AI-M12 Series versions prior to 1.2, NPort 5600-8-DT Series versions prior to 2.4, NPort 5600-8-DTL Series versions prior to 2.4, NPort 6x50 Series versions prior to 1.13.11, NPort IA5450A versions prior to v1.4. A configuration file contains parameters that represent passwords in	2017-02-13	2.1	CVE-2016-9348 BID (link is external) MISC

	plaintext.			
samsung -- samsung_mobile	Samsung devices with Android KK(4.4) or L(5.0/5.1) allow local users to cause a denial of service (IAndroidShm service crash) via crafted data in a service call.	2017-02-13	2.1	CVE-2016-4546 CONFIRM (link is external) MLIST (link is external)
wso2 -- carbon	Cross-site request forgery (CSRF) vulnerability in WSO2 Carbon 4.4.5 allows remote attackers to hijack the authentication of privileged users for requests that shutdown a server via a shutdown action to server-admin/proxy_ajaxprocessor.jsp.	2017-02-16	3.5	CVE-2016-4315 MISC MISC (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM (link is external) EXPLOIT-DB (link is external)

- 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).