National Critical Information Infrastructure Protection Centre

CVE Report

01-15 December 2016 Vol. 03 No. 21

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Adobe					
Animate Adobe Animate is a multimedia authoring and computer animation program developed by Adobe Systems.					
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe Animate versions 15.2.1.95 and earlier have exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7866**	https://helpx.adobe.com/security/products/animate/apsb16-38.html	A-ADO-ANIMA-211216/01
Cold fusion Builder Adobe ColdFusion Builder software is the only professional IDE that allows you to build and deploy web and mobile applications.					
Gain Information	15-12-2016	5	Adobe ColdFusion Builder versions 2016 update 2 and earlier, 3.0.3 and earlier have an important vulnerability that could lead to information disclosure. **REFERENCE: CVE-2016-7887**	https://helpx.adobe.com/security/products/coldfusion/apsb16-44.html	A-ADO-COLDF-211216/02
Digital Editions Most major publishers use Adobe Digital Editions (ADE) to proof-read their books.					
Gain Information	15-12-2016	5	Adobe Digital Editions versions 4.5.2 and earlier has an issue with parsing crafted XML entries that could lead to information disclosure. **REFERENCE: CVE-2016-7889**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-45.html	A-ADO-DIGIT-211216/03
Gain Information	15-12-2016	5	Adobe Digital Editions versions 4.5.2 and earlier has an important vulnerability that could lead to memory address leak.	https://helpx.adobe.com/security/products/Digital-Editions/apsb	A-ADO-DIGIT-211216/04

			REFERENCE: CVE-2016-7888	16-45.html	
Dng Converter The Adobe DNG Converter is a free utility that enables you to easily convert camera-specific raw files from more than 600 cameras to the more universal DNG raw format.					
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe DNG Converter versions 9.7 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7856**	https://helpx.adobe.com/security/products/dng-converter/apsb16-41.html	A-ADO-DNGC-211216/05
Experience Manager Adobe Experience Manager is an enterprise content management solution that helps simplify the management and delivery of your content and assets.					
Cross Site Request Forgery	15-12-2016	6.8	Adobe Experience Manager versions 6.2 and earlier have a vulnerability that could be used in Cross-Site Request Forgery attacks. **REFERENCE: CVE-2016-7885**	https://helpx.adobe.com/security/products/experience-manager/apsb16-42.html	A-ADO-EXPER-211216/06
Cross Site Scripting	15-12-2016	4.3	Adobe Experience Manager versions 6.1 and earlier have an input validation issue in the DAM create assets that could be used in cross-site scripting attacks. **REFERENCE: CVE-2016-7884**	https://helpx.adobe.com/security/products/experience-manager/apsb16-42.html	A-ADO-EXPER-211216/07
Cross Site Scripting	15-12-2016	4.3	Adobe Experience Manager version 6.2 has an input validation issue in create Launch wizard that could be used in cross-site scripting attacks. **REFERENCE: CVE-2016-7883**	https://helpx.adobe.com/security/products/experience-manager/apsb16-42.html	A-ADO-EXPER-211216/08
Cross Site Scripting	15-12-2016	4.3	Adobe Experience Manager versions 6.2 and earlier have an input validation issue in the WCMDebug filter that could be used in cross-site	https://helpx.adobe.com/security/products/experience-	A-ADO-EXPER-211216/09

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			scripting attacks. **REFERENCE: CVE-2016-7882**	manager/apsb16-42.html	
Experience Manager Forms; Live cycle Adobe Experience Manager is an enterprise content management solution that helps simplify the management and delivery of your content and assets; Adobe Live Cycle Enterprise Suite (ES4) is an SOA Java EE server software product from Adobe Systems Incorporated used to build applications that automate a broad range of business processes for enterprises and government agencies.					
Cross Site Scripting	15-12-2016	4.3	Adobe Experience Manager Forms versions 6.2 and earlier, LiveCycle 11.0.1, LiveCycle 10.0.4 have an input validation issue in the PMAdmin module that could be used in cross-site scripting attacks. **REFERENCE: CVE-2016-6934**	https://helpx.adobe.com/security/products/aem-forms/apsb16-40.html	A-ADO-EXPER-211216/10
Cross Site Scripting	15-12-2016	4.3	Adobe Experience Manager Forms versions 6.2 and earlier, LiveCycle 11.0.1, LiveCycle 10.0.4 have an input validation issue in the AACComponent that could be used in cross-site scripting attacks. **REFERENCE: CVE-2016-6933**	https://helpx.adobe.com/security/products/aem-forms/apsb16-40.html	A-ADO-EXPER-211216/11
Flash Player; Flash Player For Linux Adobe Flash Player is freeware software for using content created on the Adobe Flash platform, including viewing multimedia, executing rich Internet applications, and streaming video and audio; Flash Player is also available for Linux platform.					
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the TextField class. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7892**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/12
Bypass	15-12-2016	7.5	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have	https://helpx.adobe.com/security/produc	A-ADO-FLASH-211216/13

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			security bypass vulnerability in the implementation of the same origin policy. **REFERENCE: CVE-2016-7890**	ts/flash-player/apsb16-39.html	
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class when handling conversion to an object. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7881**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/14
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability when setting the length property of an array object. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7880**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/15
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the NetConnection class when handling an attached script object. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7879**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/16
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the PSDK's	https://helpx.adobe.com/security/products/flash-player/apsb1	A-ADO-FLASH-211216/17

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			MediaPlayer class. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7878**	6-39.html	
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the Action Message Format serialization (AFM0). Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7877**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/18
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Clipboard class related to data handling functionality. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7876**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/19
Execute Code, Overflow	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable integer overflow vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7875**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/20
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the NetConnection class when handling the proxy types.	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/21

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7874**		
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the PSDK class related to ad policy functionality method. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7873**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/22
Execute Code	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class related to objects at multiple presentation levels. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7872**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/23
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Worker class. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7871**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/24
Execute Code, Overflow	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class for specific	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/25

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			search strategies. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7870**		
Execute Code, Overflow	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to backtrack search functionality. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7869**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/26
Execute Code, Overflow	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to alternation functionality. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7868**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/27
Execute Code, Overflow	15-12-2016	10	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to bookmarking in searches. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7867**	https://helpx.adobe.com/security/products/flash-player/apsb16-39.html	A-ADO-FLASH-211216/28
InDesign; InDesign Server Adobe InDesign is a desktop publishing software application produced by Adobe Systems; Adobe InDesign CC Server software delivers a robust and scalable engine that leverages the design, layout, and typographical capabilities of InDesign CC to let you programmatically create engaging					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

automated documents.					
Execute Code, Overflow, Memory Corruption	15-12-2016	10	Adobe InDesign version 11.4.1 and earlier, Adobe InDesign Server 11.0.0 and earlier have an exploitable memory corruption vulnerability. Successful exploitation could lead to arbitrary code execution. **REFERENCE: CVE-2016-7886**	https://helpx.adobe.com/security/products/indesign/apsb16-43.html	A-ADO-INDES-211216/29
Robohelp RoboHelp is a help authoring tool (HAT) created c. 1991 by Gen Kiyooka of Blue Sky Software for the Microsoft Windows operating system.					
Cross Site Scripting	15-12-2016	4.3	Adobe RoboHelp version 2015.0.3 and earlier, RoboHelp 11 and earlier have an input validation issue that could be used in cross-site scripting attacks. **REFERENCE: CVE-2016-7891**	https://helpx.adobe.com/security/products/robohelp/apsb16-46.html	A-ADO-ROBOH-211216/30
Alcatel-lucent					
Omnivista 8770 Network Management System OmniVista Network Management System (NMS) provides a cohesive management and network wide visibility increasing IT efficiency and business agility.					
Execute Code, Bypass	03-12-2016	10	Alcatel-Lucent OmniVista 8770 2.0 through 3.0 exposes different ORBs interfaces, which can be queried using the GIOP protocol on TCP port 30024. An attacker can bypass authentication, and OmniVista invokes methods (AddJobSet, AddJob, and ExecuteNow) that can be used to run arbitrary commands on the server, with the privilege of NT AUTHORITY\SYSTEM on the server. NOTE: The discoverer states "The vendor position is to refer to the technical guidelines of the product security deployment to mitigate this issue, which	NA	A-ALC-OMNIV-211216/31

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			means applying proper firewall rules to prevent unauthorised clients to connect to the OmniVista server." **REFERENCE: CVE-2016-9796**		
Apache					
Http Server The Apache HTTP Server Project is an effort to develop and maintain an open-source HTTP server for modern operating systems including UNIX and Windows.					
Denial of Service	05-12-2016	5	The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request. **REFERENCE: CVE-2016-8740**	https://github.com/apache/httpd/commit/29c63b786ae028d82405421585e91283c8fa0da3	A-APA-HTTP -211216/32
Tika Apache Tika is a content analysis toolkit.					
Gain Information	15-12-2016	5	Apache Tika server (aka tika-server) in Apache Tika 1.9 might allow remote attackers to read arbitrary files via the HTTP fileUrl header. **REFERENCE: CVE-2015-3271**	NA	A-APA-TIKA-211216/33
Atlassian					
Crowd Atlassian's Crowd is a software application installed by the system administrator.					
Execute Code	09-12-2016	7.5	The LDAP directory connector in Atlassian Crowd before 2.8.8 and 2.9.x before 2.9.5 allows remote attackers to execute arbitrary code via an LDAP attribute with a crafted serialized Java object, aka LDAP entry poisoning.	https://confluence.atlassian.com/crowd/crowd-security-advisory-2016-10-19-856697283.ht	A-ATL-CROWD-211216/34

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-6496	ml	
B2evolution					
B2evolution B2evolution is a content and community management system written in PHP and backed by a MySQL database.					
NA	02-12-2016	5	The "lost password" functionality in b2evolution before 6.7.9 allows remote attackers to reset arbitrary user passwords via a crafted request. **REFERENCE: CVE-2016-9479**	https://github.com/b2evolution/b2evolution/issues/33	A-B2E-B2EVO-211216/35
Bdwgc Project					
Bdwgc NA					
Denial of Service, Execute Code, Overflow	11-12-2016	7.5	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation. **REFERENCE: CVE-2016-9427**	https://github.com/ivmai/bdwgc/issues/135	A-BDW-BDWGC-211216/36
Bluez					
Bluez BlueZ provides support for the core Bluetooth layers and protocols. It is flexible, efficient and uses a modular implementation.					
Overflow	03-12-2016	5	In BlueZ 5.42, a buffer overflow was observed in "commands_dump" function in "tools/parser/csr.c" source file. The issue exists because "commands" array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame "frm->ptr" parameter. This issue can be triggered by processing a corrupted dump	NA	A-BLU-BLUEZ-211216/37

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			file and will result in hcidump crash. **REFERENCE: CVE-2016-9804**		
Overflow	03-12-2016	5	In BlueZ 5.42, an out-of-bounds read was observed in "le_meta_ev_dump" function in "tools/parser/hci.c" source file. This issue exists because 'subevent' (which is used to read correct element from 'ev_le_meta_str' array) is overflowed. **REFERENCE: CVE-2016-9803**	NA	A-BLU-BLUEZ-211216/38
Overflow	03-12-2016	5	In BlueZ 5.42, a buffer over-read was identified in "l2cap_packet" function in "monitor/packet.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash. **REFERENCE: CVE-2016-9802**	NA	A-BLU-BLUEZ-211216/39
Overflow	03-12-2016	5	In BlueZ 5.42, a buffer overflow was observed in "set_ext_ctrl" function in "tools/parser/l2cap.c" source file when processing corrupted dump file. **REFERENCE: CVE-2016-9801**	NA	A-BLU-BLUEZ-211216/40
Overflow	03-12-2016	5	In BlueZ 5.42, a buffer overflow was observed in "pin_code_reply_dump" function in "tools/parser/hci.c" source file. The issue exists because "pin" array is overflowed by supplied parameter due to lack of boundary checks on size of the buffer from frame "pin_code_reply_cp *cp" parameter.	NA	A-BLU-BLUEZ-211216/41

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-9800		
Overflow	03-12-2016	5	In BlueZ 5.42, a buffer overflow was observed in "pklg_read_hci" function in "btsnoop.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash. **REFERENCE: CVE-2016-9799**	NA	A-BLU-BLUEZ-211216/42
NA	03-12-2016	5	In BlueZ 5.42, a use-after-free was identified in "conf_opt" function in "tools/parser/l2cap.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash. **REFERENCE: CVE-2016-9798**	NA	A-BLU-BLUEZ-211216/43
NA	03-12-2016	5	In BlueZ 5.42, a buffer over-read was observed in "l2cap_dump" function in "tools/parser/l2cap.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash. **REFERENCE: CVE-2016-9797**	NA	A-BLU-BLUEZ-211216/44
Bluez Project					
Bluez BlueZ provides support for the core Bluetooth layers and protocols. It is flexible, efficient and uses a modular implementation.					
NA	08-12-2016	5	In BlueZ 5.42, an out-of-bounds read was identified in "packet_hexdump" function in "monitor/packet.c" source file. This issue can be triggered by processing a corrupted dump file and will result in btmon crash. **REFERENCE: CVE-2016-**	https://www.spinics.net/lists/linux-bluetooth/msg68898.html	A-BLU-BLUEZ-211216/45

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			9918		
Overflow	08-12-2016	5	In BlueZ 5.42, a buffer overflow was observed in "read_n" function in "tools/hcidump.c" source file. This issue can be triggered by processing a corrupted dump file and will result in hcidump crash. **REFERENCE: CVE-2016-9917**	https://www.spinics.net/lists/linux-bluetooth/msg68892.html	A-BLU-BLUEZ-211216/46
BMC					
Blade Logic Server Automation Console BMC Server Automation, one of BMC's digital enterprise automation solutions, allows you to quickly and securely provision, configure, patch, and maintain physical, virtual, and cloud servers.					
Bypass	13-12-2016	7.5	BMC Blade Logic Server Automation (BSA) before 8.7 Patch 3 allows remote attackers to bypass authentication and consequently read arbitrary files or possibly have unspecified other impact by leveraging a "logic flaw" in the authentication process. **REFERENCE: CVE-2016-4322**	NA	A-BMC-BLADE-211216/47
Patrol BMC PATROL An application management suite from BMC that uses agents to report on software activities on all the servers within the enterprise.					
NA	02-12-2016	7.2	In BMC Patrol before 9.13.10.02, the binary "listguests64" is configured with the setuid bit. However, when executing it, it will look for a binary named "virsh" using the PATH environment variable. The "listguests64" program will then run "virsh" using root privileges. This allows local users to elevate their privileges to root. **REFERENCE: CVE-2016-9638**	http://www.nes.fr/securitylab/index.php/2016/12/02/privilege-escalation-on-bmc-patrol	A-BMC-PATRO-211216/48

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Busybox					
Busybox BusyBox is software that provides several stripped-down Unix tools in a single executable file.					
Denial of Service	09-12-2016	7.8	The recv_and_process_client_pkt function in networking/ntpd.c in busybox allows remote attackers to cause a denial of service (CPU and bandwidth consumption) via a forged NTP packet, which triggers a communication loop. **REFERENCE: CVE-2016-6301**	https://bugzilla.redhat.com/show_bug.cgi?id=1363710	A-BUS-BUSYB-211216/49
Cisco					
AnyConnect Secure Mobility Client The 3.1 version of Cisco AnyConnect Secure Mobility Client for Mac is provided as a free download on our website.					
NA	13-12-2016	7.2	Vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to install and execute an arbitrary executable file with privileges equivalent to the Microsoft Windows operating system SYSTEM account. More Information: CSCvb68043. Known Affected Releases: 4.3(2039) 4.3(748). Known Fixed Releases: 4.3(4019) 4.4(225). **REFERENCE: CVE-2016-9192**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-anyconnect1	A-CIS-ANYCO-211216/50
Asr 5000 Series Software Cisco ASR 5000 Series is architected to address the anticipated increase in performance requirements that the next generation of the mobile Internet will bring.					
Overflow	13-12-2016	5	A vulnerability in the Internet Key Exchange Version 2 (IKEv2) feature of Cisco ASR 5000 Series Software could allow an unauthenticated, remote attacker to cause a reload of the ipsecmgr process. More Information:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-asr1	A-CIS-ASR 5-211216/51

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			CSCvb38398. Known Affected Releases: 20.2.3 20.2.3.65026. Known Fixed Releases: 21.1.M0.65431 21.1.PP0.65733 21.1.R0.65467 21.1.R0.65496 21.1.VC0.65434 21.1.VC0.65489 21.2.A0.65437. **REFERENCE: CVE-2016-9203**		
NA	13-12-2016	5	Vulnerability in IPv6 packet fragment reassembly of StarOS for Cisco Aggregation Services Router (ASR) 5000 Series Switch could allow an unauthenticated, remote attacker to cause an unexpected reload of the Network Processing Unit (NPU) process. More Information: CSCva84552. Known Affected Releases: 20.0.0 21.0.0 21.0.M0.64702. Known Fixed Releases: 21.0.0 21.0.0.65256 21.0.M0.64970 21.0.V0.65150 21.1.A0.64973 21.1.PP0.65270 21.1.R0.65130 21.1.R0.65135 21.1.VC0.65203. **REFERENCE: CVE-2016-6467**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-asr	A-CIS-ASR 5-211216/52
Content Security Management Appliance; Email Security Appliance; Web Security Appliance The Cisco Content Security Management Appliance complements all of the Cisco Email and Web Security Appliances; Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats; The Cisco Web Security Appliance (WSA) combines all forms of protection and more in a single solution.					
NA	13-12-2016	4.3	Vulnerability in the update functionality of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA), Cisco Web Security Appliance (WSA), and Cisco Content Management Security Appliance (SMA) could allow	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-asyncos	A-CIS-CONTE-211216/53

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			an unauthenticated, remote attacker to impersonate the update server. More Information: CSCul88715, CSCul94617, CSCul94627. Known Affected Releases: 7.5.2-201 7.6.3-025 8.0.1-023 8.5.0-000 8.5.0-ER1-198 7.5.2-HP2-303 7.7.0-608 7.7.5-835 8.5.1-021 8.8.0-000 7.9.1-102 8.0.0-404 8.1.1-013 8.2.0-222. Known Fixed Releases: 8.0.2-069 8.0.2-074 8.5.7-042 9.1.0-032 8.5.2-027 9.6.1-019. **REFERENCE: CVE-2016-1411**		
Email Security Appliance Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats					
Cross-site scripting	13-12-2016	4.3	Vulnerability in the web-based management interface of Cisco Email Security Appliance (ESA) Switches could allow an unauthenticated, remote attacker to conduct a persistent cross-site scripting (XSS) attack against a user of the affected interface on an affected device. More Information: CSCvb37346. Known Affected Releases: 9.1.1-036 9.7.1-066. **REFERENCE: CVE-2016-9202**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-esa1	A-CIS-EMAIL-211216/54
Bypass	13-12-2016	4.3	Vulnerability in the content filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances and Cisco Web Security Appliances could allow an unauthenticated, remote attacker to bypass user filters that are configured for an	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-esa	A-CIS-EMAIL-211216/55

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			affected device. Affected Products: This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for both virtual and hardware versions of the following Cisco products: Cisco Email Security Appliances (ESAs) that are configured to use message or content filters that scan incoming email attachments; Cisco Web Security Appliances (WSAs) that are configured to use services that scan accessed web content. More Information: CSCva90076, CSCvb06764. Known Affected Releases: 10.0.0-125 8.5.7-042 9.7.2-047. **REFERENCE: CVE-2016-6465**		
Emergency Responder Cisco Emergency Responder enhances the existing emergency 9-1-1 functionality offered by Cisco Unified Communications Manager (previously known as Cisco Unified Call Manager).					
Directory Traversal	13-12-2016	4	Vulnerability in the File Management Utility, the Download File form, and the Serviceability application of Cisco Emergency Responder could allow an authenticated, remote attacker to access files in arbitrary locations on the file system of an affected device. More Information: CSCva98951 CSCva98954 CSCvb57494. Known Affected Releases: 11.5(2.10000.5). Known Fixed Releases: 12.0(0.98000.14) 12.0(0.98000.16). **REFERENCE: CVE-2016-9208**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-cer1	A-CIS-EMERG-211216/56
Cross Site	13-12-2016	6.8	Vulnerability in the web-	https://tools.c	A-CIS-

Request Forgery			based management interface of Cisco Emergency Responder could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. More Information: CSCvb06663. Known Affected Releases: 11.5(1.10000.4). Known Fixed Releases: 12.0(0.98000.14). **REFERENCE: CVE-2016-6468**	isco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-cer	EMERG-211216/57
Expressway Cisco Expressway advanced collaboration gateways for unified communications promotes simple and secure collaboration anywhere, on any device.					
NA	13-12-2016	6.4	Vulnerability in the HTTP traffic server component of Cisco Expressway could allow an unauthenticated, remote attacker to initiate TCP connections to arbitrary hosts. This does not allow for full traffic proxy through the Expressway. Affected Products: This vulnerability affects Cisco Expressway Series Software and Cisco TelePresence Video Communication Server (VCS). More Information: CSCvc10834. Known Affected Releases: X8.7.2 X8.8.3. Known Fixed Releases: X8.9. **REFERENCE: CVE-2016-9207**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-expressway	A-CIS-EXPRE-211216/58
Fireamp Connector Endpoint Software NA					
Denial of Service	13-12-2016	4.6	Vulnerability in the system management of certain FireAMP system processes in Cisco FireAMP Connector Endpoint software could	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory	A-CIS-FIREA-211216/59

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			allow an authenticated, local attacker to stop certain protected FireAMP processes without requiring a password. Stopping certain critical processes could cause a denial of service (DoS) condition, and certain security features could no longer be available. More Information: CSCvb40597. Known Affected Releases: 1. **REFERENCE: CVE-2016-6449**	y/cisco-sa-20161207-fireamp	
Firepower Management Center; Firesight System Software This is your administrative nerve center for managing critical Cisco network security solutions.					
Bypass	13-12-2016	5	Vulnerability in the malicious file detection and blocking features of Cisco Firepower Management Center and Cisco FireSIGHT System Software could allow an unauthenticated, remote attacker to bypass malware detection mechanisms on an affected system. Affected Products: Cisco Firepower Management Center and FireSIGHT System Software are affected when they are configured to use a file policy that has the Block Malware action. More Information: CSCvb27494. Known Affected Releases: 6.0.1.1 6.1.0. **REFERENCE: CVE-2016-9193**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-firepower	A-CIS-FIREP-211216/60
Firepower Services For Adaptive Security Appliance Cisco ASA with FirePOWER Services delivers an integrated threat defense across the entire attack continuum — before, during, and after an attack.					
NA	13-12-2016	4.3	Vulnerability in TCP processing in Cisco FirePOWER system software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-FIREP-211216/61

			attacker to download files that would normally be blocked. Affected Products: The following Cisco products are vulnerable: Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services, Advanced Malware Protection (AMP) for Networks - 7000 Series Appliances, Advanced Malware Protection (AMP) for Networks - 8000 Series Appliances, FirePOWER 7000 Series Appliances, FirePOWER 8000 Series Appliances, FirePOWER Threat Defense for Integrated Services Routers (ISRs), Next Generation Intrusion Prevention System (NGIPS) for Blue Coat X-Series, Sourcefire 3D System Appliances, Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware. More Information: CSCvb20102. Known Affected Releases: 2.9.7.10. **REFERENCE: CVE-2016-9209**	y/cisco-sa-20161207-fpwr	
Firesight System In a passive IPS deployment, the FireSIGHT System monitors traffic flowing across a network using a switch SPAN or mirror port.					
Gain Information	13-12-2016	4	A vulnerability in the web-based management interface of Cisco Firepower Management Center running FireSIGHT System software could allow an authenticated, remote attacker to view the Remote Storage Password. More Information: CSCvb19366. Known Affected	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-vdc	A-CIS-FIRES-211216/62

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Releases: 5.4.1.6. **REFERENCE: CVE-2016-6471**		
Hybrid Media Service Cisco Spark Hybrid Media Service offer a simple, secure, powerful way to connect on-premises and cloud services, delivering superior audio, video, and content sharing.					
NA	13-12-2016	7.2	Vulnerability in the installation procedure of the Cisco Hybrid Media Service could allow an authenticated, local attacker to elevate privileges to the root level. More Information: CSCvb81344. Known Affected Releases: 1.0. **REFERENCE: CVE-2016-6470**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-hms	A-CIS-HYBRI-211216/63
Identity Services Engine ISE gives you a next-generation NAC solution that offers guest access, profiling, and BYOD.					
Denial of Service	13-12-2016	5	A vulnerability in the Active Directory integration component of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to perform a denial of service (DoS) attack. More Information: CSCuw15041. Known Affected Releases: 1.2(1.199). **REFERENCE: CVE-2016-9198**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ise	A-CIS-IDENT-211216/64
Identity Services Engine Software ISE gives you a next-generation NAC solution that offers guest access, profiling, and BYOD. They are enforced by role-based software-defined segmentation.					
Cross Site Scripting	13-12-2016	4.3	Cisco Identity Services Engine (ISE) contains a vulnerability that could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface of the affected system. More Information: CSCvb86332 CSCvb86760. Known Affected Releases:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ise1	A-CIS-IDENT-211216/65

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			2.0(101.130). **REFERENCE: CVE-2016-9214**		
IOX Cisco IOx offers consistent management and hosting across network infrastructure products, including Cisco routers, switches, and compute modules.					
Directory Traversal	13-12-2016	6.8	A vulnerability in the Cisco application-hosting framework (CAF) of Cisco IOX could allow an authenticated, remote attacker to read arbitrary files on a targeted system. Affected Products: This vulnerability affects specific releases of the Cisco IOx subsystem of Cisco IOS and IOS XE Software. More Information: CSCvb23331. Known Affected Releases: 15.2(6.0.57i)E CAF-1.1.0.0. **REFERENCE: CVE-2016-9199**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-caf	A-CIS-IOX-211216/66
Nexus 1000v Intercloud Firmware Cisco Nexus 1000V InterCloud provides the architectural foundation for secure hybrid clouds, allowing enterprises to easily and securely connect the enterprise data center to the public cloud.					
NA	13-12-2016	6.4	Vulnerability in the Cisco Intercloud Fabric (ICF) Director could allow an unauthenticated, remote attacker to connect to internal services with an internal account. Affected Products: Cisco Nexus 1000V InterCloud is affected. More Information: CSCus99379. Known Affected Releases: 2.2(1). **REFERENCE: CVE-2016-9204**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-icf	A-CIS-NEXUS-211216/67
Ons 15454 Sdh Multiservice Platform Software NA					
NA	13-12-2016	5	A vulnerability in TCP port management in Cisco ONS 15454 Series Multiservice Provisioning Platforms could allow an unauthenticated,	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisor	A-CIS-ONS1-211216/68

			remote attacker to cause the controller card to unexpectedly reload. More Information: CSCuw26032. Known Affected Releases: 10.51. **REFERENCE: CVE-2016-9211**	y/cisco-sa-20161207-cons	
Prime Collaboration Assurance Cisco Prime Collaboration is a comprehensive video and voice service assurance and management system					
Cross Site Scripting	13-12-2016	4.3	A vulnerability in the web framework code of Cisco Prime Collaboration Assurance could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against the user of the web interface. More Information: CSCut43268. Known Affected Releases: 10.5(1) 10.6. **REFERENCE: CVE-2016-9200**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-pca	A-CIS-PRIME-211216/69
Unified Communications Manager Cisco Unified Communications Manager is an enterprise-class IP telephony call-processing system.					
Directory Traversal	13-12-2016	5	Vulnerability in the Cisco Unified Reporting upload tool accessed via the Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to modify arbitrary files on the file system. More Information: CSCvb61698. Known Affected Releases: 11.5(1.11007.2). Known Fixed Releases: 12.0(0.98000.168) 12.0(0.98000.178) 12.0(0.98000.399) 12.0(0.98000.510) 12.0(0.98000.536) 12.0(0.98500.7). **REFERENCE: CVE-2016-9210**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-cur	A-CIS-UNIFI-211216/70

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Cross Site Scripting	13-12-2016	4.3	Vulnerability in the ccmadmin page of Cisco Unified Communications Manager (CUCM) could allow an unauthenticated, remote attacker to conduct reflected cross-site scripting (XSS) attacks. More Information: CSCvb64641. Known Affected Releases: 11.5(1.10000.6) 11.5(1.11007.2). Known Fixed Releases: 11.5(1.12900.7) 11.5(1.12900.8) 12.0(0.98000.155) 12.0(0.98000.178) 12.0(0.98000.366) 12.0(0.98000.468) 12.0(0.98000.536) 12.0(0.98500.6). **REFERENCE: CVE-2016-9206**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-cucm	A-CIS-UNIFI-211216/71
Unified Communications Manager Im and Presence Service Cisco Unified Communications Manager is an enterprise-class IP telephony call-processing system.					
Gain Information	13-12-2016	5	Vulnerability in the web management interface of the Cisco Unified Communications Manager IM and Presence Service could allow an unauthenticated, remote attacker to view information on web pages that should be restricted. More Information: CSCva49629. Known Affected Releases: 11.5(1). Known Fixed Releases: 11.5(1.12000.2) 12.0(0.98000.181). **REFERENCE: CVE-2016-6464**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ucm	A-CIS-UNIFI-211216/72
Web Security Appliance The Cisco Web Security Appliance (WSA) combines all of these forms of protection and more in a single solution.					
NA	13-12-2016	5	Vulnerability in the Decrypt for End-User Notification	https://tools.cisco.com/secu	A-CIS-WEBS-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			configuration parameter of Cisco AsyncOS Software for Cisco Web Security Appliances could allow an unauthenticated, remote attacker to connect to a secure website over Secure Sockets Layer (SSL) or Transport Layer Security (TLS), even if the WSA is configured to block connections to the website. Affected Products: This vulnerability affects Cisco Web Security Appliances if the HTTPS decryption options are enabled and configured for the device to block connections to certain websites. More Information: CSCvb49012. Known Affected Releases: 9.0.1-162 9.1.1-074. **REFERENCE: CVE-2016-9212**	rity/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-wsa1	211216/73
Denial of Service	13-12-2016	5	Vulnerability in HTTP URL parsing of Cisco AsyncOS for Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) vulnerability due to the proxy process unexpectedly restarting. More Information: CSCvb04312. Known Affected Releases: 9.0.1-162 9.1.1-074. Known Fixed Releases: 10.1.0-129 9.1.2-010. **REFERENCE: CVE-2016-6469**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-wsa	A-CIS-WEBS-211216/74
Crowbar Project					
Barclamp-trove; Crowbar-openstack Crowbar was the first open source OpenStack-focused deployment framework.					
NA	09-12-2016	7.5	The trove service user in (1) Openstack deployment (aka	https://www.suse.com/sec	A-CRO-BARCL-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			crowbar-openstack) and (2) Trove Barclamp (aka barclamp-trove and crowbar-barclamp-trove) in the Crowbar Framework has a default password, which makes it easier for remote attackers to obtain access via unspecified vectors. **REFERENCE: CVE-2016-6829**	urity/cve//REFERENCE: CVE-2016-6829.html	211216/75
Dotclear					
Dotclear Dotclear is an open source blog publishing application distributed under the GNU GPLv2.					
Cross Site Scripting	09-12-2016	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the media manager in Dotclear before 2.10 allow remote attackers to inject arbitrary web script or HTML via the (1) q or (2) link_type parameter to admin/media.php. **REFERENCE: CVE-2016-6523**	https://hg.dotclear.org/dotclear/file/18dc878c1178/CHANGELOG	A-DOT-DOTCL-211216/76
Gnome					
Libgsf libgsf is a simple i/o library that can read and write common file types and handle structured formats that provide file-system-in-a-file semantics.					
NA	08-12-2016	4.3	An error within the "tar_directory_for_file()" function (gsf-infile-tar.c) in GNOME Structured File Library before 1.14.41 can be exploited to trigger a Null pointer deReference and subsequently cause a crash via a crafted TAR file. **REFERENCE: CVE-2016-9888**	NA	A-GNO-LIBGS-211216/77
GNU					
TAR GNU Tar provides the ability to create tar archives, as well as various other kinds of manipulation.					
Directory	09-12-2016	5	Directory traversal	http://git.sav	A-GNU-TAR-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Traversal, Bypass			vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER. **REFERENCE: CVE-2016-6321**	annah.gnu.org/cgit/tar.git/commit/?id=7340f67b9860ea0531c1450e5aa261c50f67165d	211216/78
IBM					
Api Connect; Network Path Manager IBM API Connect is an API management solution that addresses critical aspects of the API lifecycle for both on-premises and cloud environments.					
Bypass, Gain Information	01-12-2016	5	IBM API Connect (aka APIConnect) before 5.0.3.0 with NPM before 2.2.8 includes certain internal server credentials in the software package, which might allow remote attackers to bypass intended access restrictions by leveraging knowledge of these credentials. **REFERENCE: CVE-2016-3012**	http://www-01.ibm.com/support/docview.wss?uid=swg21988212	A-IBM-APIC-211216/79
Appscan Source IBM Security AppScan Source helps organizations lower costs and reduce risk exposure by identifying web-based and mobile application source code vulnerabilities early in the software development lifecycle, so they can be fixed before deployment.					
Denial of Service	01-12-2016	5.5	IBM AppScan Source 8.7 through 9.0.3.3 allows remote authenticated users to read arbitrary files or cause a denial of service (memory consumption) via an XML document containing an external entity declaration in conjunction with an entity Reference, related to an XML External Entity (XXE) issue.	http://www-01.ibm.com/support/docview.wss?uid=swg21987326	A-IBM-APPSC-211216/80

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-3033		
Connections IBM Connections Suite provides IBM social solutions, including software, real-time social communications and content management capabilities.					
Cross Site Scripting	01-12-2016	3.5	Cross-site scripting (XSS) vulnerability in IBM Connections 5.0 before CR4 and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **REFERENCE: CVE-2016-2955**	http://www-01.ibm.com/support/docview.wss?uid=swg21988531	A-IBM-CONNE-211216/81
Filenet Workplace Workplace XT is an optional FileNet P8 platform component (similar to Application Engine) that hosts the Workplace XT web application.					
Denial of Service	01-12-2016	5.5	IBM FileNet Workplace 4.0.2 before 4.0.2.14 LA012 allows remote authenticated users to read arbitrary files or cause a denial of service (memory consumption) via an XML document containing an external entity declaration in conjunction with an entity Reference, related to an XML External Entity (XXE) issue. **REFERENCE: CVE-2016-3055**	http://www-01.ibm.com/support/docview.wss?uid=swg21987128	A-IBM-FILEN-211216/82
NA	01-12-2016	4.9	Open redirect vulnerability in IBM FileNet Workplace 4.0.2 through 4.0.2.14 IF001 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **REFERENCE: CVE-2016-3047**	http://www-01.ibm.com/support/docview.wss?uid=swg21987126	A-IBM-FILEN-211216/83
Lotus Protector For Mail Security Lotus Protector for Mail Security IBM's preemptive protective and spam control for Lotus Domino.					
Cross Site Scripting	01-12-2016	3.5	Multiple cross-site scripting (XSS) vulnerabilities in IBM Lotus Protector for Mail	http://www-01.ibm.com/support/docvi	A-IBM-LOTUS-211216/84

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Security 2.8.0.0 through 2.8.1.0 before 2.8.1.0-22115 allow remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **REFERENCE: CVE-2016-2991**	ew.wss?uid=swg21985280	
Powerkvm PowerKVM – the open virtualization choice for Power scale-out Linux Systems.					
Denial of Service	01-12-2016	4.9	The Linux kernel component in IBM PowerKVM 2.1 before 2.1.1.3-65.10 and 3.1 before 3.1.0.2 allows guest OS users to cause a denial of service (host OS infinite loop and hang) via unspecified vectors. **REFERENCE: CVE-2016-3044**	http://www-01.ibm.com/support/docview.wss?uid=isg3T1023969	A-IBM-POWER-211216/85
Tivoli Monitoring IBM Tivoli Monitoring products monitor the performance and availability of distributed operating systems and applications.					
Overflow ,Gain Privileges	01-12-2016	7.2	Stack-based buffer overflow in the ax Shared Libraries in the Agent in IBM Tivoli Monitoring (ITM) 6.2.2 before FP9, 6.2.3 before FP5, and 6.3.0 before FP2 on Linux and UNIX allows local users to gain privileges via unspecified vectors. **REFERENCE: CVE-2016-2946**	http://www-01.ibm.com/support/docview.wss?uid=swg21984578	A-IBM-TIVOL-211216/86
Urban code Deploy IBM Urban Code Deploy is a tool for automating application deployments through your environments.					
Cross Site Scripting	01-12-2016	3.5	Cross-site scripting (XSS) vulnerability in IBM UrbanCode Deploy 6.2.x before 6.2.1.2 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **REFERENCE: CVE-2016-2994**	http://www-01.ibm.com/support/docview.wss?uid=swg2C1000177	A-IBM-URBAN-211216/87

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

IBM; Pcre					
Powerkvm/Pcre The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5.					
Denial of Service, Overflow Bypass ,Gain Information	13-12-2016	6.4	Heap-based buffer overflow in the find_fixedlength function in pcre_compile.c in PCRE before 8.38 allows remote attackers to cause a denial of service (crash) or obtain sensitive information from heap memory and possibly bypass the ASLR protection mechanism via a crafted regular expression with an excess closing parenthesis. **REFERENCE: CVE-2015-5073**	http://www-01.ibm.com/support/docview.wss?uid=isg3T1023886	A-IBM-POWER-211216/88
Powerkvm /Pcre; Pcre2 IBM PowerKVM is an open virtualization solution that is offered for the Power scale-out family of Linux servers built on POWER8 technology/The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5; PCRE2 is short for Perl Compatible Regular Expressions, version 2.					
Denial of Service, Overflow	13-12-2016	5	PCRE 7.8 and 8.32 through 8.37, and PCRE2 10.10 mishandle group empty matches, which might allow remote attackers to cause a denial of service (stack-based buffer overflow) via a crafted regular expression, as demonstrated by /^(?:(?(1)\\.|([^\\\\W_])?)+)+$/. **REFERENCE: CVE-2015-3217**	https://bugs.exim.org/show_bug.cgi?id=1638	A-IBM-POWER-211216/89
Imagemagick					
Imagemagick ImageMagick is a software suite to create, edit, compose, or convert bitmap images.					
Overflow	13-12-2016	6.4	Buffer overflow in MagickCore/enhance.c in ImageMagick before 7.0.2-7 allows remote attackers to have unspecified impact via	https://github.com/ImageMagick/ImageMagick/commit/76401e172e	A-IMA-IMAGE-211216/90

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			vectors related to pixel cache morphology. **REFERENCE: CVE-2016-6520**	a3a55182be2b8e2aca4d07270f6da6	
Intel					
Proset/wireless Software And Drivers Intel PROSet Wireless Intel is the driver necessary for handling wireless networks/ Intel Wireless Software and Drivers is included download options for driver-only and driver-with Intel PROSet/Wireless Software.					
Denial of Service, Overflow	08-12-2016	2.1	Buffer overflow in Intel PROSet/Wireless Software and Drivers in versions before 19.20.3 allows a local user to crash iframewrk.exe causing a potential denial of service. **REFERENCE: CVE-2016-8104**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00065&languageid=en-fr	A-INT-PROSE-211216/91
Wireless Bluetooth Drivers NA					
	08-12-2016	7.2	Unquoted service path vulnerability in Intel Wireless Bluetooth Drivers 16.x, 17.x, and before 18.1.1607.3129 allows local users to launch processes with elevated privileges. **REFERENCE: CVE-2016-8102**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00059&languageid=en-fr	A-INT-WIREL-211216/92
Jfrog					
Artifactory JFrog Artifactory is a Universal Artifact Repository.					
Execute Code	09-12-2016	7.5	JFrog Artifactory before 4.11 allows remote attackers to execute arbitrary code via an LDAP attribute with a crafted serialized Java object, aka LDAP entry poisoning. **REFERENCE: CVE-2016-6501**	https://www.jfrog.com/confluence/display/RTF/Release+Notes#ReleaseNotes-MainUpdates.7	A-JFR-ARTIF-211216/93
Joomla					
Joomla! Joomla! is the mobile-ready and user-friendly way to build your website.					
NA	05-12-2016	7.5	The file scanning mechanism	NA	A-JOO-

			of JFilterInput::isFileSafe() in Joomla! CMS before 3.6.5 does not consider alternative PHP file extensions when checking uploaded files for PHP content, which enables a user to upload and execute files with the `.php6`, `.php7`, `.phtml`, and `.phpt` extensions. Additionally, JHelperMedia::canUpload() did not blacklist these file extensions as uploadable file types. **REFERENCE: CVE-2016-9836**		JOOML-211216/94
Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
Denial of Service, Overflow ,Gain Information	06-12-2016	5.8	Integer overflow in tools/bmp2tiff.c in LibTIFF before 4.0.4 allows remote attackers to cause a denial of service (heap-based buffer over-read), or possibly obtain sensitive information from process memory, via crafted width and length values in RLE4 or RLE8 data in a BMP file. **REFERENCE: CVE-2015-8870**	http://download.osgeo.org/libtiff/tiff-4.0.4.tar.gz	A-LIB-LIBTI-211216/95
Mailcwp Project					
Mailcwp MailCWP is designed to be responsive and feature rich. Powered by jQuery and AJAX the system responds quickly to user requests.					
NA	14-12-2016	7.5	Mailcwp remote file upload vulnerability incomplete fix v1.100 **REFERENCE: CVE-2016-1000156**	NA	A-MAI-MAILC-211216/96
Mariadb; Mysql; Wolfssl					
Mariadb/Mysql/Wolfssl NA					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

NA	13-12-2016	2.1	The C software implementation of AES Encryption and Decryption in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover AES keys by leveraging cache-bank timing differences. **REFERENCE: CVE-2016-7440**	https://wolfssl.com/wolfSSL/Blog/Entries/2016/9/26_wolfSSL_3.9.10_Vulnerability_Fixes.html	A-MAR-MARIA-211216/97
Mariadb; Oracle; Percona					
Mariadb/Mysql/Percona Server; Xtradb Cluster NA					
Gain Privileges	13-12-2016	6.9	mysqld_safe in Oracle MySQL through 5.5.51, 5.6.x through 5.6.32, and 5.7.x through 5.7.14; MariaDB; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17, when using file-based logging, allows local users with access to the mysql account to gain root privileges via a symlink attack on error logs and possibly other files. **REFERENCE: CVE-2016-6664**	https://www.percona.com/blog/2016/11/02/percona-responds-to-Reference: CVE-2016-6663-and-Reference: CVE-2016-6664/	A-MAR-MARIA-211216/98
Nagios					
Nagios Nagios provides enterprise-class Open Source IT monitoring, network monitoring, server and applications monitoring.					
Gain Privileges	15-12-2016	7.2	base/logging.c in Nagios Core before 4.2.4 allows local users with access to an account in the nagios group to gain root privileges via a symlink attack on the log file. NOTE: this can be leveraged	https://bugzilla.redhat.com/show_bug.cgi?id=1402869	A-NAG-NAGIO-211216/99

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			by remote attackers using CVE-2016-9565. **REFERENCE: CVE-2016-9566**		
NA	15-12-2016	7.5	MagpieRSS, as used in the front-end component in Nagios Core before 4.2.2 might allow remote attackers to read or write to arbitrary files by spoofing a crafted response from the Nagios RSS feed server. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4796. **REFERENCE: CVE-2016-9565**	https://www.nagios.org/projects/nagios-core/history/4x/	A-NAG-NAGIO-211216/100
Naver					
Ngrinder nGrinder is a platform for stress tests that enables you to execute script creation, test execution, monitoring, and result report generator simultaneously.					
Cross Site Scripting	13-12-2016	4.3	Multiple cross-site scripting (XSS) vulnerabilities in nGrinder before 3.4 allow remote attackers to inject arbitrary web script or HTML via the (1) description, (2) email, or (3) username parameter to user/save. **REFERENCE: CVE-2016-5060**	https://github.com/naver/ngrinder/issues/103	A-NAV-NGRIN-211216/101
Netapp					
Netapp Plug-in NetApp Virtual Storage Console (VSC) for VMware vSphere provides integrated, end-to-end virtual storage management for your VMware infrastructure.					
NA	05-12-2016	6.8	NetApp Plug-in for Symantec NetBackup prior to version 2.0.1 makes use of a non-unique server certificate, making it vulnerable to impersonation. **REFERENCE: CVE-2016-7171**	https://kb.netapp.com/support/s/article/NTAP-20161129-0001	A-NET-NETAP-211216/102
Openbsd					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Openssh OpenSSH, also known as OpenBSD Secure Shell, is a suite of security-related network-level utilities based on the SSH protocol, which help to secure network communications via the encryption of network traffic over multiple authentication methods and by providing secure tunneling capabilities.					
Denial of Service	09-12-2016	7.8	** DISPUTED ** The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests. NOTE: a third party reports that "OpenSSH upstream does not consider this as a security issue." **REFERENCE: CVE-2016-8858**	NA	A-OPE-OPENS-211216/103
Open-xchange					
Open-xchange Appsuite *OX App Suite* includes a set of applications that are meant for email, contacts, calendars, media and all documents.					
Gain Information	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. Users can provide local file paths to the RSS reader; the response and error code give hints about whether the provided file exists or not. Attackers may discover specific system files or library versions on the middleware server to prepare further attacks. **REFERENCE: CVE-2016-6852**	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/104
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. SVG files can be used as profile pictures. In case their XML structure contains iframes and script code, that code may get executed when calling the related picture	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/105

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			URL or viewing the related person's image within a browser. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6850**		
Execute Code	15-12-2016	1.9	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. API requests can be used to inject, generate and download executable files to the client ("Reflected File Download"). Malicious platform specific (e.g. Microsoft Windows) batch file can be created via a trusted domain without authentication that, if executed by the user, may lead to local code execution. **REFERENCE: CVE-2016-6848**	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/106
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. SVG files can be used as mp3 album covers. In case their XML structure contains script code, that code may get executed when calling the related cover URL. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.).	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/107

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			REFERENCE: CVE-2016-6847		
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. Script code within hyperlinks at HTML E-Mails is not getting correctly sanitized when using base64 encoded "data" resources. This allows an attacker to provide hyperlinks that may execute script code instead of directing to a proper location. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6845**	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/108
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. Script code within SVG files is maintained when opening such files "in browser" based on our Mail or Drive app. In case of "a" tags, this may include link targets with base64 encoded "data" References. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6844**	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/109
Execute Code, Cross-site	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite	https://software.open-	A-OPE-OPEN--

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

scripting			before 7.8.2-rev8. Script code can be injected to contact names. When adding those contacts to a group, the script code gets executed in the context of the user which creates or changes the group by using autocomplete. In most cases this is a user with elevated permissions. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6843**	xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	211216/110
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev8. Setting the user's name to JS code makes that code execute when selecting that user's "Templates" folder from OX Documents settings. This requires the folder to be shared to the victim. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6842**	https://software.open-xchange.com/OX6/6.22/doc/Release_Notes_for_Patch_Release_3522_7.8.2_2016-08-29.pdf	A-OPE-OPEN--211216/111
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.2-rev5. JavaScript code can be used as part of ical attachments within	http://packetstormsecurity.com/files/138700/Open-Xchange-App-	A-OPE-OPEN--211216/112

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			scheduling E-Mails. This content, for example an appointment's location, will be presented to the user at the E-Mail App, depending on the invitation workflow. This code gets executed within the context of the user's current session. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-5740**	Suite-7.8.2-Cross-Site-Scripting.html	
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev14. Adding images from external sources to HTML editors by drag&drop can potentially lead to script code execution in the context of the active user. To exploit this, a user needs to be tricked to use an image from a specially crafted website and add it to HTML editor areas of OX App Suite, for example E-Mail Compose or OX Text. This specific attack circumvents typical XSS filters and detection mechanisms since the code is not loaded from an external service but injected locally. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data	http://www.securityfocus.com/archive/1/archive/1/538892/100/0/threaded	A-OPE-OPEN--211216/113

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			etc.). To exploit this vulnerability, a attacker needs to convince a user to follow specific steps (social-engineering). **REFERENCE: CVE-2016-5124**		
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev11. Script code can be embedded to RSS feeds using a URL notation. In case a user clicks the corresponding link at the RSS reader of App Suite, code gets executed at the context of the user. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). The attacker needs to reside within the same context to make this attack work. **REFERENCE: CVE-2016-4045**	http://www.securityfocus.com/archive/1/archive/1/538732/100/0/threaded	A-OPE-OPEN--211216/114
Gain Information	15-12-2016	3.5	An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev10. App Suite frontend offers to control whether a user wants to store cookies that exceed the session duration. This functionality is useful when logging in from clients with reduced privileges or shared environments. However the setting was incorrectly recognized and cookies were stored regardless of this setting when the login was performed using a non-	http://packetstormsecurity.com/files/137599/Open-Xchange-App-Suite-7.8.1-Information-Disclosure.html	A-OPE-OPEN--211216/115

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			interactive login method. In case the setting was enforced by middleware configuration or the user went through the interactive login page, the workflow was correct. Cookies with authentication information may become available to other users on shared environments. In case the user did not properly log out from the session, third parties with access to the same client can access a user's account. **REFERENCE: CVE-2016-4027**		
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX App Suite before 7.8.1-rev11. The content sanitizer component has an issue with filtering malicious content in case invalid HTML code is provided. In such cases the filter will output a unsanitized representation of the content. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). Attackers can use this issue for filter evasion to inject script code later on. **REFERENCE: CVE-2016-4026**	http://www.securityfocus.com/archive/1/archive/1/538732/100/0/threaded	A-OPE-OPEN--211216/116
NA	15-12-2016	4.3	An issue was discovered in Open-Xchange OX AppSuite before 7.8.0-rev27. The "defer" servlet offers to redirect a client to a specified URL. Since some checks were	http://packetstormsecurity.com/files/137187/Open-Xchange-OX-AppSuite-	A-OPE-OPEN--211216/117

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			missing, arbitrary URLs could be provided as redirection target. Users can be tricked to follow a link to a trustworthy domain but end up at an unexpected service later on. This vulnerability can be used to prepare and enhance phishing attacks. **REFERENCE: CVE-2016-3174**	7.8.0-XSS-Open-Redirect.html	
Execute Code, Cross-site scripting	15-12-2016	3.5	An issue was discovered in Open-Xchange OX AppSuite before 7.8.0-rev27. The aria-label parameter of tiles at the Portal can be used to inject script code. Those labels use the name of the file (e.g. an image) which gets displayed at the portal application. Using script code at the file name leads to script execution. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). Users actively need to add a file to the portal to enable this attack. In case of shared files however, a internal attacker may modify a previously embedded file to carry a malicious file name. Furthermore this vulnerability can be used to persistently execute code that got injected by a temporary script execution vulnerability. **REFERENCE: CVE-2016-3173**	http://www.securityfocus.com/archive/1/archive/1/538481/100/0/threaded	A-OPE-OPEN--211216/118

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange Server 6 / OX AppSuite before 7.8.0-rev26. The "session" parameter for file-download requests can be used to inject script code that gets reflected through the subsequent status page. Malicious script code can be executed within a trusted domain's context. While no OX App Suite specific data can be manipulated, the vulnerability can be exploited without being authenticated and therefore used for social engineering attacks, stealing cookies or redirecting from trustworthy to malicious hosts. **REFERENCE: CVE-2016-2840**	http://packetstormsecurity.com/files/136543/Open-Xchange-7.8.0-Cross-Site-Scripting.html	A-OPE-OPEN--211216/119
Ox Guard OX Guard is designed to make security for email and files seamless and simple and in making things simple, Open-Xchange makes security work.					
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX Guard before 2.4.2-rev5. Script code which got injected to a mail with inline PGP signature gets executed when verifying the signature. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6854**	http://www.securityfocus.com/archive/1/archive/1/539395/100/0/threaded	A-OPE-OX GU-211216/120
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX Guard before 2.4.2-rev5. Script code and References to external	http://www.securityfocus.com/archive/1/archive/1/5	A-OPE-OX GU-211216/121

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			websites can be injected to the names of PGP public keys. When requesting that key later on using a specific URL, such script code might get executed. In case of injecting external websites, users might get lured into a phishing scheme. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.). **REFERENCE: CVE-2016-6853**	39395/100/0/threaded	
Execute Code, Cross-site scripting	15-12-2016	4.3	An issue was discovered in Open-Xchange OX Guard before 2.4.2-rev5. Script code can be provided as parameter to the OX Guard guest reader web application. This allows cross-site scripting attacks against arbitrary users since no prior authentication is needed. Malicious script code can be executed within a user's context. This can lead to session hijacking or triggering unwanted actions via the web interface (sending mail, deleting data etc.) in case the user has an active session on the same domain already. **REFERENCE: CVE-2016-6851**	http://packetstormsecurity.com/files/138701/Open-Xchange-Guard-2.4.2-Cross-Site-Scripting.html	A-OPE-OX GU-211216/122
NA	15-12-2016	3.5	An issue was discovered in Open-Xchange OX Guard before 2.4.0-rev8. OX Guard uses an authentication token to identify and transfer guest	http://www.securityfocus.com/archive/1/archive/1/538732/100/0	A-OPE-OX GU-211216/123

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			users credentials. The OX Guard API acts as a padding oracle by responding with different error codes depending on whether the provided token matches the encryption padding. In combination with AES-CBC, this allows attackers to guess the correct padding. Attackers may run brute-forcing attacks on the content of the guest authentication token and discover user credentials. For a practical attack vector, the guest users needs to have logged in, the content of the guest user's "OxReaderID" cookie and the value of the "auth" parameter needs to be known to the attacker. **REFERENCE: CVE-2016-4028**	/threaded	
NA	15-12-2016	4	An issue was discovered in Open-Xchange Guard before 2.2.0-rev8. The "getprivkeybyid" API call is used to download a PGP Private Key for a specific user after providing authentication credentials. Clients provide the "id" and "cid" parameter to specify the current user by its user- and context-ID. The "auth" parameter contains a hashed password string which gets created by the client by asking the user to enter his or her OX Guard password. This parameter is used as single point of authentication when accessing PGP Private Keys. In case a user has set	http://www.securityfocus.com/archive/1/archive/1/537678/100/0/threaded	A-OPE-OX GU-211216/124

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			the same password as another user, it is possible to download another user's PGP Private Key by iterating the "id" and "cid" parameters. This kind of attack would also be able by brute-forcing login credentials, but since the "id" and "cid" parameters are sequential they are much easier to predict than a user's login name. At the same time, there are some obvious insecure standard passwords that are widely used. A attacker could send the hashed representation of typically weak passwords and randomly fetch Private Key of matching accounts. The attack can be executed by both internal users and "guests" which use the external mail reader. **REFERENCE: CVE-2015-8542**		
Pcre					
Pcre;Pcre2 The PCRE library is a set of functions that implement regular expression pattern matching using the same syntax and semantics as Perl 5; The newest version, PCRE2, was released in 2015 and is at version 10.22.					
Execute Code, Overflow	13-12-2016	7.5	Heap-based buffer overflow in PCRE 8.34 through 8.37 and PCRE2 10.10 allows remote attackers to execute arbitrary code via a crafted regular expression, as demonstrated by /^(?P=B)((?P=B)(?J:(?P<B>c)(?P<B>a(?P=B)))>WGXCREDITS)/, a different vulnerability than CVE-2015-8384. **REFERENCE: CVE-2015-3210**	https://bugs.exim.org/show_bug.cgi?id=1636	A-PCR-PCRE;-211216/125

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Phpmyadmin					
Phpmyadmin phpMyAdmin is a free and open source tool written in PHP intended to handle the administration of MySQL with the use of a web browser.					
Cross Site Request Foregery	10-12-2016	6.8	An issue was discovered in phpMyAdmin. When the arg_separator is different from its default & value, the CSRF token was not properly stripped from the return URL of the pReference import action. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9866**	https://www.phpmyadmin.net/security/PMASA-2016-71	A-PHP-PHPMY-211216/126
Bypass	10-12-2016	7.5	An issue was discovered in phpMyAdmin. Due to a bug in serialized string parsing, it was possible to bypass the protection offered by PMA_safeUnserialize() function. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9865**	https://www.phpmyadmin.net/security/PMASA-2016-70	A-PHP-PHPMY-211216/127
SQL Injection	10-12-2016	6	An issue was discovered in phpMyAdmin. With a crafted username or a table name, it was possible to inject SQL statements in the tracking functionality that would run with the privileges of the control user. This gives read and write access to the tables of the configuration storage database, and if the control user has the necessary privileges, read access to some tables of the MySQL	https://www.phpmyadmin.net/security/PMASA-2016-69	A-PHP-PHPMY-211216/128

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			database. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9864**		
Denial of Service	10-12-2016	5	An issue was discovered in phpMyAdmin. With a very large request to table partitioning function, it is possible to invoke a Denial of Service (DoS) attack. All 4.6.x versions (prior to 4.6.5) are affected. **REFERENCE: CVE-2016-9863**	https://www.phpmyadmin.net/security/PMASA-2016-68	A-PHP-PHPMY-211216/129
Bypass	10-12-2016	5	An issue was discovered in phpMyAdmin. Due to the limitation in URL matching, it was possible to bypass the URL white-list protection. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9861**	https://www.phpmyadmin.net/security/PMASA-2016-66	A-PHP-PHPMY-211216/130
Denial of Service	10-12-2016	4.3	An issue was discovered in phpMyAdmin. An unauthenticated user can execute a denial of service attack when phpMyAdmin is running with $cfg['AllowArbitraryServer']=true. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9860**	https://www.phpmyadmin.net/security/PMASA-2016-65	A-PHP-PHPMY-211216/131
Denial of Service	10-12-2016	5	An issue was discovered in phpMyAdmin. With a crafted	https://www.phpmyadmin.	A-PHP-PHPMY-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			request parameter value it is possible to initiate a denial of service attack in import feature. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9859**	net/security/ PMASA-2016-65	211216/132
Denial of Service	10-12-2016	5	An issue was discovered in phpMyAdmin. With a crafted request parameter value it is possible to initiate a denial of service attack in saved searches feature. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9858**	https://www.phpmyadmin.net/security/ PMASA-2016-65	A-PHP-PHPMY-211216/133
Cross Site Scripting	10-12-2016	4.3	An issue was discovered in phpMyAdmin. XSS is possible because of a weakness in a regular expression used in some JavaScript processing. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9857**	https://www.phpmyadmin.net/security/ PMASA-2016-64	A-PHP-PHPMY-211216/134
Cross Site Scripting	10-12-2016	4.3	An XSS issue was discovered in phpMyAdmin because of an improper fix for REFERENCE: CVE-2016-2559 in PMASA-2016-10. This issue is resolved by using a copy of a hash to avoid a race condition. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior	https://www.phpmyadmin.net/security/ PMASA-2016-64	A-PHP-PHPMY-211216/135

			to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9856**		
Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the PMA_shutdownDuringExport issue. **REFERENCE: CVE-2016-9855**	https://www.phpmyadmin.net/security/PMASA-2016-63	A-PHP-PHPMY-211216/136
Execute Code ,Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of	https://www.phpmyadmin.net/security/PMASA-2016-63	A-PHP-PHPMY-211216/137

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the json_decode issue. **REFERENCE: CVE-2016-9854**		
Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the fopen wrapper issue. **REFERENCE: CVE-2016-9853**	https://www.phpmyadmin.net/security/PMASA-2016-63	A-PHP-PHPMY-211216/138
Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. By calling some scripts that are part of phpMyAdmin in an unexpected way, it is possible to trigger phpMyAdmin to display a PHP error message which contains the full path of the directory where phpMyAdmin is installed. During an execution timeout	https://www.phpmyadmin.net/security/PMASA-2016-63	A-PHP-PHPMY-211216/139

			in the export functionality, the errors containing the full path of the directory of phpMyAdmin are written to the export file. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. This CVE is for the curl wrapper issue. **REFERENCE: CVE-2016-9852**		
Bypass	10-12-2016	5	An issue was discovered in phpMyAdmin. With a crafted request parameter value it is possible to bypass the logout timeout. All 4.6.x versions (prior to 4.6.5), and 4.4.x versions (prior to 4.4.15.9) are affected. **REFERENCE: CVE-2016-9851**	https://www.phpmyadmin.net/security/PMASA-2016-62	A-PHP-PHPMY-211216/140
Bypass	10-12-2016	7.5	An issue was discovered in phpMyAdmin. It is possible to bypass AllowRoot restriction ($cfg['Servers'][$i]['AllowRoot']) and deny rules for username by using Null Byte in the username. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9849**	https://www.phpmyadmin.net/security/PMASA-2016-60	A-PHP-PHPMY-211216/141
Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. phpinfo (phpinfo.php) shows PHP information including values of HttpOnly cookies. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions	https://www.phpmyadmin.net/security/PMASA-2016-59	A-PHP-PHPMY-211216/142

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			(prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9848**		
NA	10-12-2016	5	An issue was discovered in phpMyAdmin. When the user does not specify a blowfish_secret key for encrypting cookies, phpMyAdmin generates one at runtime. A vulnerability was reported where the way this value is created uses a weak algorithm. This could allow an attacker to determine the user's blowfish_secret and potentially decrypt their cookies. All 4.6.x versions (prior to 4.6.5), 4.4.x versions (prior to 4.4.15.9), and 4.0.x versions (prior to 4.0.10.18) are affected. **REFERENCE: CVE-2016-9847**	https://www.phpmyadmin.net/security/PMASA-2016-58	A-PHP-PHPMY-211216/143
Execute Code	10-12-2016	6.8	An issue was discovered in phpMyAdmin. phpMyAdmin can be used to trigger a remote code execution attack against certain PHP installations that are running with the dbase extension. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6633**	https://www.phpmyadmin.net/security/PMASA-2016-56	A-PHP-PHPMY-211216/144
NA	10-12-2016	4.3	An issue was discovered in phpMyAdmin where, under certain conditions, phpMyAdmin may not delete temporary files during the import of ESRI files. All 4.6.x	https://www.phpmyadmin.net/security/PMASA-2016-55	A-PHP-PHPMY-211216/145

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6632**		
Execute Code	10-12-2016	8.5	An issue was discovered in phpMyAdmin. A user can execute a remote code execution attack against a server when phpMyAdmin is being run as a CGI application. Under certain server configurations, a user can pass a query string which is executed as a command-line argument by the file generator_plugin.sh. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6631**	https://www.phpmyadmin.net/security/PMASA-2016-54	A-PHP-PHPMY-211216/146
NA	10-12-2016	4	An issue was discovered in phpMyAdmin. An authenticated user can trigger a denial-of-service (DoS) attack by entering a very long password at the change password dialog. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6630**	https://www.phpmyadmin.net/security/PMASA-2016-53	A-PHP-PHPMY-211216/147
Bypass	10-12-2016	10	An issue was discovered in phpMyAdmin involving the $cfg['ArbitraryServerRegexp'] configuration directive. An attacker could reuse certain	https://www.phpmyadmin.net/security/PMASA-2016-52	A-PHP-PHPMY-211216/148

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			cookie values in a way of bypassing the servers defined by ArbitraryServerRegexp. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6629**		
NA	10-12-2016	6.8	An issue was discovered in phpMyAdmin. An attacker may be able to trigger a user to download a specially crafted malicious SVG file. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6628**	https://www.phpmyadmin.net/security/PMASA-2016-51	A-PHP-PHPMY-211216/149
Gain Information	10-12-2016	5	An issue was discovered in phpMyAdmin. An attacker can determine the phpMyAdmin host location through the file url.php. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6627**	https://www.phpmyadmin.net/security/PMASA-2016-50	A-PHP-PHPMY-211216/150
NA	10-12-2016	5.8	An issue was discovered in phpMyAdmin. An attacker could redirect a user to a malicious web page. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-**	https://www.phpmyadmin.net/security/PMASA-2016-49	A-PHP-PHPMY-211216/151

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			6626		
Gain Information	10-12-2016	4	An issue was discovered in phpMyAdmin. An attacker can determine whether a user is logged in to phpMyAdmin. The user's session, username, and password are not compromised by this vulnerability. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6625**	https://www.phpmyadmin.net/security/PMASA-2016-48	A-PHP-PHPMY-211216/152
NA	10-12-2016	4.3	An issue was discovered in phpMyAdmin involving improper enforcement of the IP-based authentication rules. When phpMyAdmin is used with IPv6 in a proxy server environment, and the proxy server is in the allowed range but the attacking computer is not allowed, this vulnerability can allow the attacking computer to connect despite the IP rules. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6624**	https://www.phpmyadmin.net/security/PMASA-2016-47	A-PHP-PHPMY-211216/153
Bypass	10-12-2016	4	An issue was discovered in phpMyAdmin. An authorized user can cause a denial-of-service (DoS) attack on a server by passing large values to a loop. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to	https://www.phpmyadmin.net/security/PMASA-2016-46	A-PHP-PHPMY-211216/154

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6623**		
NA	10-12-2016	4.3	An issue was discovered in phpMyAdmin. An unauthenticated user is able to execute a denial-of-service (DoS) attack by forcing persistent connections when phpMyAdmin is running with $cfg['AllowArbitraryServer'] =true. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6622**	https://www.phpmyadmin.net/security/PMASA-2016-45	A-PHP-PHPMY-211216/155
Execute Code	10-12-2016	7.5	An issue was discovered in phpMyAdmin. Some data is passed to the PHP unserialize() function without verification that it's valid serialized data. The unserialization can result in code execution because of the interaction with object instantiation and autoloading. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6620**	https://www.phpmyadmin.net/security/PMASA-2016-43	A-PHP-PHPMY-211216/156
SQL Injection	10-12-2016	6.5	An issue was discovered in phpMyAdmin. In the user interface pReference feature, a user can execute an SQL injection attack against the account of the control user. All 4.6.x versions (prior to	https://www.phpmyadmin.net/security/PMASA-2016-42	A-PHP-PHPMY-211216/157

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6619**		
NA	10-12-2016	4	An issue was discovered in phpMyAdmin. The transformation feature allows a user to trigger a denial-of-service (DoS) attack against the server. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6618**	https://www.phpmyadmin.net/security/PMASA-2016-41	A-PHP-PHPMY-211216/158
SQL Injection	10-12-2016	6.8	An issue was discovered in phpMyAdmin. A specially crafted database and/or table name can be used to trigger an SQL injection attack through the export functionality. All 4.6.x versions (prior to 4.6.4) are affected. **REFERENCE: CVE-2016-6617**	https://www.phpmyadmin.net/security/PMASA-2016-40	A-PHP-PHPMY-211216/159
SQL Injection	10-12-2016	6.8	An issue was discovered in phpMyAdmin. In the "User group" and "Designer" features, a user can execute an SQL injection attack against the account of the control user. All 4.6.x versions (prior to 4.6.4) and 4.4.x versions (prior to 4.4.15.8) are affected. **REFERENCE: CVE-2016-6616**	https://www.phpmyadmin.net/security/PMASA-2016-39	A-PHP-PHPMY-211216/160
Cross-site scripting	10-12-2016	4.3	XSS issues were discovered in phpMyAdmin. This affects navigation pane and	https://www.phpmyadmin.net/security/	A-PHP-PHPMY-211216/161

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			database/table hiding feature (a specially-crafted database name can be used to trigger an XSS attack); the "Tracking" feature (a specially-crafted query can be used to trigger an XSS attack); and GIS visualization feature. All 4.6.x versions (prior to 4.6.4) and 4.4.x versions (prior to 4.4.15.8) are affected. **REFERENCE: CVE-2016-6615**	PMASA-2016-38	
Directory Traversal	10-12-2016	4.3	An issue was discovered in phpMyAdmin involving the %u username replacement functionality of the SaveDir and UploadDir features. When the username substitution is configured, a specially-crafted user name can be used to circumvent restrictions to traverse the file system. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6614**	https://www.phpmyadmin.net/security/PMASA-2016-37	A-PHP-PHPMY-211216/162
Gain Information	10-12-2016	2.1	An issue was discovered in phpMyAdmin. A user can specially craft a symlink on disk, to a file which phpMyAdmin is permitted to read but the user is not, which phpMyAdmin will then expose to the user. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-**	https://www.phpmyadmin.net/security/PMASA-2016-36	A-PHP-PHPMY-211216/163

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			6613		
Gain Information	10-12-2016	4	An issue was discovered in phpMyAdmin. A user can exploit the LOAD LOCAL INFILE functionality to expose files on the server to the database system. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6612**	https://www.phpmyadmin.net/security/PMASA-2016-35	A-PHP-PHPMY-211216/164
SQL Injection	10-12-2016	5.1	An issue was discovered in phpMyAdmin. A specially crafted database and/or table name can be used to trigger an SQL injection attack through the export functionality. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6611**	https://www.phpmyadmin.net/security/PMASA-2016-34	A-PHP-PHPMY-211216/165
Gain Information	10-12-2016	4	A full path disclosure vulnerability was discovered in phpMyAdmin where a user can trigger a particular error in the export mechanism to discover the full path of phpMyAdmin on the disk. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6610**	https://www.phpmyadmin.net/security/PMASA-2016-33	A-PHP-PHPMY-211216/166
NA	10-12-2016	6.5	An issue was discovered in phpMyAdmin. A specially crafted database name could	https://www.phpmyadmin.net/security/	A-PHP-PHPMY-211216/167

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			be used to run arbitrary PHP commands through the array export feature. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6609**	PMASA-2016-32	
Cross-site scripting	10-12-2016	4.3	XSS issues were discovered in phpMyAdmin. This affects the database privilege check and the "Remove partitioning" functionality. Specially crafted database names can trigger the XSS attack. All 4.6.x versions (prior to 4.6.4) are affected. **REFERENCE: CVE-2016-6608**	https://www.phpmyadmin.net/security/PMASA-2016-31	A-PHP-PHPMY-211216/168
Cross-site scripting	10-12-2016	4.3	XSS issues were discovered in phpMyAdmin. This affects Zoom search (specially crafted column content can be used to trigger an XSS attack); GIS editor (certain fields in the graphical GIS editor are not properly escaped and can be used to trigger an XSS attack); Relation view; the following Transformations: Formatted, Imagelink, JPEG: Upload, RegexValidation, JPEG inline, PNG inline, and transformation wrapper; XML export; MediaWiki export; Designer; When the MySQL server is running with a specially-crafted log_bin directive; Database tab; Replication feature; and Database search. All 4.6.x versions (prior to 4.6.4),	https://www.phpmyadmin.net/security/PMASA-2016-30	A-PHP-PHPMY-211216/169

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6607**		
NA	10-12-2016	5	An issue was discovered in cookie encryption in phpMyAdmin. The decryption of the username/password is vulnerable to a padding oracle attack. This can allow an attacker who has access to a user's browser cookie file to decrypt the username and password. Furthermore, the same initialization vector (IV) is used to hash the username and password stored in the phpMyAdmin cookie. If a user has the same password as their username, an attacker who examines the browser cookie can see that they are the same - but the attacker can not directly decode these values from the cookie as it is still hashed. All 4.6.x versions (prior to 4.6.4), 4.4.x versions (prior to 4.4.15.8), and 4.0.x versions (prior to 4.0.10.17) are affected. **REFERENCE: CVE-2016-6606**	https://www.phpmyadmin.net/security/PMASA-2016-29	A-PHP-PHPMY-211216/170
NA	10-12-2016	3.6	An issue was discovered in phpMyAdmin. A user can be tricked into following a link leading to phpMyAdmin, which after authentication redirects to another malicious site. The attacker must sniff the user's valid phpMyAdmin token. All 4.0.x	https://www.phpmyadmin.net/security/PMASA-2016-57	A-PHP-PHPMY-211216/171

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			versions (prior to 4.0.10.16) are affected. **REFERENCE: CVE-2016-4412**		
Piwigo					
Piwigo Piwigo is photo gallery software for the web, built by an active community of users and developers.					
Cross-site scripting	01-12-2016	4.3	Cross-site scripting (XSS) vulnerability in the search results front end in Piwigo 2.8.3 allows remote attackers to inject arbitrary web script or HTML via the search parameter. **REFERENCE: CVE-2016-9751**	https://github.com/Piwigo/Piwigo/issues/559	A-PIW-PIWIG-211216/172
PWC					
Ace-advanced Business Application Programming ABAP (Advanced Business Application Programming) is a programming language for developing applications for the SAP R/3 system, a widely-installed business application subsystem.					
Execute Code	09-12-2016	6.5	PricewaterhouseCoopers (PwC) ACE-ABAP 8.10.304 for SAP Security allows remote authenticated users to conduct ABAP injection attacks and execute arbitrary code via (1) SAPGUI or (2) Internet Communication Framework (ICF) over HTTP or HTTPS, as demonstrated by WEBGUI or Report. **REFERENCE: CVE-2016-9832**	NA	A-PWC-ACE-A-211216/173
Qemu					
Qemu QEMU is a generic and open source machine emulator and virtualizer.					
Denial of Service	09-12-2016	2.1	Memory leak in the v9fs_write function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) by leveraging failure to free an	http://git.qemu.org/?p=qemu.git;a=commit;h=fdfcc9aeea1492f4b819a24c94dfb678145b1bf9	A-QEM-QEMU-211216/174

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			IO vector. **REFERENCE: CVE-2016-9106**		
Denial of Service	09-12-2016	2.1	Memory leak in the v9fs_link function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via vectors involving a Reference to the source fid object. **REFERENCE: CVE-2016-9105**	http://git.qemu.org/?p=qemu.git;a=commit;h=4c1586787ff43c9acd18a56c12d720e3e6be9f7c	A-QEM-QEMU-211216/175
Denial of Service, Overflow	09-12-2016	2.1	Multiple integer overflows in the (1) v9fs_xattr_read and (2) v9fs_xattr_write functions in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS administrators to cause a denial of service (QEMU process crash) via a crafted offset, which triggers an out-of-bounds access. **REFERENCE: CVE-2016-9104**	NA	A-QEM-QEMU-211216/176
Overflow ,Gain Information	09-12-2016	2.1	The v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host heap memory information by reading xattribute values before writing to them. **REFERENCE: CVE-2016-9103**	http://git.qemu.org/?p=qemu.git;a=commit;h=eb687602853b4ae656e9236ee4222609f3a6887d	A-QEM-QEMU-211216/177
Denial of Service	09-12-2016	2.1	Memory leak in the v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) via a	http://git.qemu.org/?p=qemu.git;a=commit;h=ff55e94d23ae94c8628b0115320157c763eb3e06	A-QEM-QEMU-211216/178

			large number of Txattrcreate messages with the same fid number. **REFERENCE: CVE-2016-9102**		
Denial of Service	09-12-2016	2.1	Memory leak in hw/net/eepro100.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by repeatedly unplugging an i8255x (PRO100) NIC device. **REFERENCE: CVE-2016-9101**	NA	A-QEM-QEMU-211216/179
Denial of Service	09-12-2016	2.1	Memory leak in the ehci_process_itd function in hw/usb/hcd-ehci.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via a large number of crafted buffer page select (PG) indexes. **REFERENCE: CVE-2016-7995**	http://git.qemu.org/?p=qemu.git;a=commit;h=b16c129daf0fed91febbb88de23dae8271c8898a	A-QEM-QEMU-211216/180
Denial of Service	09-12-2016	2.1	Memory leak in the virtio_gpu_resource_create_2d function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_CREATE_2D commands. **REFERENCE: CVE-2016-7994**	NA	A-QEM-QEMU-211216/181
Denial of Service	09-12-2016	2.1	Memory leak in the usb_xhci_exit function in hw/usb/hcd-xhci.c in QEMU	http://git.qemu.org/?p=qemu.git;a=commi	A-QEM-QEMU-211216/182

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			(aka Quick Emulator), when the xhci uses msix, allows local guest OS administrators to cause a denial of service (memory consumption and possibly QEMU process crash) by repeatedly unplugging a USB device. **REFERENCE: CVE-2016-7466**	t;h=b53dd4495ced2432a0b652ea895e651d07336f7e	
Denial of Service	09-12-2016	2.1	The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer deReference and QEMU process crash) via a large I/O descriptor buffer length value. **REFERENCE: CVE-2016-7422**	http://git.qemu.org/?p=qemu.git;a=commit;h=973e7170dddefb491a48df5cba33b2ae151013a0	A-QEM-QEMU-211216/183
Denial of Service	09-12-2016	2.1	The pvscsi_ring_pop_req_descr function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit process IO loop to the ring size. **REFERENCE: CVE-2016-7421**	http://git.qemu.org/?p=qemu.git;a=commit;h=d251157ac1928191af851d199a9ff255d330bec9	A-QEM-QEMU-211216/184
Denial of Service	09-12-2016	2.1	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to cursor.mask[] and	http://git.qemu.org/?p=qemu.git;a=commit;h=167d97a3def77ee2dbf6e908b0ecbfe2103977db	A-QEM-QEMU-211216/185

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			cursor.image[] array sizes when processing a DEFINE_CURSOR svga command. **REFERENCE: CVE-2016-7170**		
Denial of Service	09-12-2016	2.1	The (1) mptsas_config_manufacturing_1 and (2) mptsas_config_ioc_0 functions in hw/scsi/mptconfig.c in QEMU (aka Quick Emulator) allow local guest OS administrators to cause a denial of service (QEMU process crash) via vectors involving MPTSAS_CONFIG_PACK. **REFERENCE: CVE-2016-7157**	http://git.qemu.org/?p=qemu.git;a=commit;h=65a8e1f6413a0f6f79894da710b5d6d43361d27d	A-QEM-QEMU-211216/186
Denial of Service	09-12-2016	2.1	The pvscsi_convert_sglist function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging an incorrect cast. **REFERENCE: CVE-2016-7156**	http://git.qemu.org/?p=qemu.git;a=commit;h=49adc5d3f8c6bb75e55ebfeab109c5c37dea65e8	A-QEM-QEMU-211216/187
Denial of Service	09-12-2016	2.1	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds access or infinite loop, and QEMU process crash) via a crafted page count for descriptor rings. **REFERENCE: CVE-2016-7155**	http://git.qemu.org/?p=qemu.git;a=commit;h=7f61f4690dd153be98900a2a508b88989e692753	A-QEM-QEMU-211216/188
Directory	09-12-2016	2.1	Directory traversal	http://git.qem	A-QEM-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Traversal			vulnerability in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to access host files outside the export path via a .. (dot dot) in an unspecified string. **REFERENCE: CVE-2016-7116**	u.org/?p=qemu.git;a=commit;h=56f101ecce0eafd09e2daf1c4eeb1377d6959261	QEMU-211216/189
Denial of Service, Overflow	09-12-2016	2.1	Integer overflow in the net_tx_pkt_init function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU process crash) via the maximum fragmentation count, which triggers an unchecked multiplication and NULL pointer deReference. **REFERENCE: CVE-2016-6888**	http://git.qemu.org/?p=qemu.git;a=commit;h=47882fa4975bf0b58dd74474329fdd7154e8f04c	A-QEM-QEMU-211216/190
Gain Information	09-12-2016	2.1	The vmxnet3_complete_packet function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host memory information by leveraging failure to initialize the txcq_descr object. **REFERENCE: CVE-2016-6836**	http://git.qemu.org/?p=qemu.git;a=commit;h=fdda170e50b8af062cf5741e12c4fb5e57a2eacf	A-QEM-QEMU-211216/191
Denial of Service, Overflow	09-12-2016	2.1	The vmxnet_tx_pkt_parse_headers function in hw/net/vmxnet_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (buffer over-read) by leveraging	http://git.qemu.org/?p=qemu.git;a=commit;h=93060258ae748573ca7197204125a2670047896d	A-QEM-QEMU-211216/192

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			failure to check IP header length. **REFERENCE: CVE-2016-6835**		
Denial of Service	09-12-2016	2.1	The net_tx_pkt_do_sw_fragmentation function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a zero length for the current fragment length. **REFERENCE: CVE-2016-6834**	http://git.qemu.org/?p=qemu.git;a=commit;h=ead315e43ea0c2ca3491209c6c8db8ce3f2bbe05	A-QEM-QEMU-211216/193
Denial of Service	09-12-2016	2.1	Use-after-free vulnerability in the vmxnet3_io_bar0_write function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU instance crash) by leveraging failure to check if the device is active. **REFERENCE: CVE-2016-6833**	http://git.qemu.org/?p=qemu.git;a=commit;h=6c352ca9b4ee3e1e286ea9e8434bd8e69ac7d0d8	A-QEM-QEMU-211216/194
Denial of Service	09-12-2016	2.1	The virtqueue_map_desc function in hw/virtio/virtio.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a zero length for the descriptor buffer. **REFERENCE: CVE-2016-6490**	http://git.qemu.org/?p=qemu.git;a=commit;h=1e7aed70144b4673fc26e73062064b6724795e5f	A-QEM-QEMU-211216/195
Denial of Service	09-12-2016	4.9	The mptsas_fetch_requests function in hw/scsi/mptsas.c in QEMU (aka Quick Emulator) allows local guest	http://git.qemu.org/?p=qemu.git;a=commit;h=06630554	A-QEM-QEMU-211216/196

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			OS administrators to cause a denial of service (infinite loop, and CPU consumption or QEMU process crash) via vectors involving s->state. **REFERENCE: CVE-2016-4964**	ccbdd25780aa03c3548aaff1eb56dffd	
Redhat					
Enterprise Virtualization Red Hat Virtualization (RHV) is an enterprise virtualization product produced by Red Hat, based on the KVM hypervisor.					
Gain Information	14-12-2016	2.1	Red Hat Enterprise Virtualization (RHEV) Manager 3.6 allows local users to obtain encryption keys, certificates, and other sensitive information by reading the engine-setup log file. **REFERENCE: CVE-2016-4443**	https://bugzilla.redhat.com/show_bug.cgi?id=1335106	A-RED-ENTER-211216/197
Roundcube					
Webmail Webmail (or web-based email) is any email client implemented as a web application running on a web server.					
Execute Code	08-12-2016	6	steps/mail/sendmail.inc in Roundcube before 1.1.7 and 1.2.x before 1.2.3, when no SMTP server is configured and the sendmail program is enabled, does not properly restrict the use of custom envelope-from addresses on the sendmail command line, which allows remote authenticated users to execute arbitrary code via a modified HTTP request that sends a crafted e-mail message. **REFERENCE: CVE-2016-9920**	https://roundcube.net/news/2016/11/28/updates-1.2.3-and-1.1.7-released	A-ROU-WEBMA-211216/198
S9Y					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Serendipity Serendipity is a PHP-powered weblog engine which gives the user an easy way to maintain a blog.					
Bypass	01-12-2016	5	In Serendipity before 2.0.5, an attacker can bypass SSRF protection by using a malformed IP address (e.g., http://127.1) or a 30x (aka Redirection) HTTP status code. **REFERENCE: CVE-2016-9752**	https://blog.s9y.org/archives/271-Serendipity-2.0.5-and-2.1-beta3-released.html	A-S9Y-SEREN-211216/199
SAP					
Download Manager SAP Download Manager is a Java application offered by SAP that allows downloading software packages and support notes.					
Gain Information	14-12-2016	1.9	SAP Download Manager 2.1.142 and earlier generates an encryption key from a small key space on Windows and Mac systems, which allows context-dependent attackers to obtain sensitive configuration information by leveraging knowledge of a hardcoded key in the program code and a computer BIOS serial number, aka SAP Security Note 2282338. **REFERENCE: CVE-2016-3685**	NA	A-SAP-DOWNL-211216/200
Gain Information	14-12-2016	1.9	SAP Download Manager 2.1.142 and earlier uses a hardcoded encryption key to protect stored data, which allows context-dependent attackers to obtain sensitive configuration information by leveraging knowledge of this key, aka SAP Security Note 2282338. **REFERENCE: CVE-2016-3684**	NA	A-SAP-DOWNL-211216/201

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Siemens					
Sicam Pas NA					
Denial of Service, Execute Code	05-12-2016	7.5	A vulnerability in Siemens SICAM PAS (all versions including V8.08) could allow a remote attacker to cause a Denial of Service condition and potentially lead to unauthenticated remote code execution by sending specially crafted packets sent to port 19234/TCP. **REFERENCE: CVE-2016-9157**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-946325.pdf	A-SIE-SICAM-211216/202
NA	05-12-2016	7.5	A vulnerability in Siemens SICAM PAS (all versions including V8.08) could allow a remote attacker to upload, download, or delete files in certain parts of the file system by sending specially crafted packets to port 19235/TCP. **REFERENCE: CVE-2016-9156**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-946325.pdf	A-SIE-SICAM-211216/203
Spip					
Spip SPIP, a publishing system SPIP is a publishing system for the Internet.					
Cross-site scripting	05-12-2016	4.3	Cross-site scripting (XSS) vulnerability in ecrire/exec/plonger.php in SPIP 3.1.3 allows remote attackers to inject arbitrary web script or HTML via the rac parameter. **REFERENCE: CVE-2016-9152**	https://core.spip.net/projects/spip/repository/revisions/23290	A-SPI-SPIP-211216/204
UMN					
Mapserver MapServer is an open source development environment for building spatially enabled internet applications.					
Gain	08-12-2016	5	In MapServer before 7.0.3,	https://github	A-UMN-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Information			OGR driver error messages are too verbose and may leak sensitive information if data connection fails. **REFERENCE: CVE-2016-9839**	.com/mapserver/mapserver/pull/5356	MAPSE-211216/205
W3m Project					
W3M W3M is a terminal web browser for Linux.					
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (infinite loop and resource consumption) via a crafted HTML page. **REFERENCE: CVE-2016-9633**	https://github.com/tats/w3m/issues/23	A-W3M-W3M-211216/206
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (global buffer overflow and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9632**	https://github.com/tats/w3m/issues/43	A-W3M-W3M-211216/207
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9631**	https://github.com/tats/w3m/issues/42	A-W3M-W3M-211216/208
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service	https://github.com/tats/w3m/issues/41	A-W3M-W3M-211216/209

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			(global buffer overflow and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9630**		
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9629**	https://github.com/tats/w3m/issues/40	A-W3M-W3M-211216/210
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9628**	https://github.com/tats/w3m/issues/39	A-W3M-W3M-211216/211
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (heap buffer overflow and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9627**	https://github.com/tats/w3m/issues/38	A-W3M-W3M-211216/212
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page. **REFERENCE: CVE-2016-9626**	https://github.com/tats/w3m/issues/37	A-W3M-W3M-211216/213

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page. **REFERENCE: CVE-2016-9625**	https://github.com/tats/w3m/issues/36	A-W3M-W3M-211216/214
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9624**	https://github.com/tats/w3m/issues/35	A-W3M-W3M-211216/215
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9623**	https://github.com/tats/w3m/issues/33	A-W3M-W3M-211216/216
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9622**	https://github.com/tats/w3m/issues/32	A-W3M-W3M-211216/217
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service	https://github.com/tats/w3m/issues/28	A-W3M-W3M-211216/218

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			(segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9443**		
Overflow; Memory Corruption	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause memory corruption in certain conditions via a crafted HTML page. **REFERENCE: CVE-2016-9442**	https://github.com/tats/w3m/commit/d43527cfa0dbb3ccefec4a6f7b32c1434739aa29	A-W3M-W3M-211216/219
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9441**	https://github.com/tats/w3m/issues/24	A-W3M-W3M-211216/220
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9440**	https://github.com/tats/w3m/issues/22	A-W3M-W3M-211216/221
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page. **REFERENCE: CVE-2016-9439**	https://github.com/tats/w3m/issues/20	A-W3M-W3M-211216/222
Denial of	11-12-2016	4.3	An issue was discovered in	https://github	A-W3M-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Service			the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9438**	.com/tats/w3m/issues/18	W3M-211216/223
Denial of Service, Overflow, Memory Corruption	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) and possibly memory corruption via a crafted HTML page. **REFERENCE: CVE-2016-9437**	https://github.com/tats/w3m/issues/17	A-W3M-W3M-211216/224
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9434**	https://github.com/tats/w3m/issues/15	A-W3M-W3M-211216/225
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (out-of-bounds array access) via a crafted HTML page. **REFERENCE: CVE-2016-9433**	https://github.com/tats/w3m/issues/14	A-W3M-W3M-211216/226
Denial of Service, Overflow, Memory Corruption	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (memory corruption,	https://github.com/tats/w3m/issues/13	A-W3M-W3M-211216/227

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			segmentation fault, and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9432**		
Denial of Service, Overflow	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page. **REFERENCE: CVE-2016-9431**	https://github.com/tats/w3m/issues/10	A-W3M-W3M-211216/228
Denial of Service	11-12-2016	4.3	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page. **REFERENCE: CVE-2016-9430**	https://github.com/tats/w3m/issues/7	A-W3M-W3M-211216/229
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Buffer overflow in the formUpdateBuffer function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9429**	https://github.com/tats/w3m/issues/29	A-W3M-W3M-211216/230
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly	https://github.com/tats/w3m/issues/26	A-W3M-W3M-211216/231

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9428**		
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Integer overflow vulnerability in the renderTable function in w3m allows remote attackers to cause a denial of service (OOM) and possibly execute arbitrary code due to bdwgc's bug (REFERENCE: CVE-2016-9427) via a crafted HTML page. **REFERENCE: CVE-2016-9426**	https://github.com/tats/w3m/issues/25	A-W3M-W3M-211216/232
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9425**	https://github.com/tats/w3m/issues/21	A-W3M-W3M-211216/233
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m doesn't properly validate the value of tag attribute, which allows remote attackers to cause a denial of service (heap buffer overflow crash) and possibly execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9424**	https://github.com/tats/w3m/issues/12	A-W3M-W3M-211216/234
Denial of Service,	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m	https://github.com/tats/w3	A-W3M-W3M-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Execute Code, Overflow			fork before 0.5.3-31. Heap-based buffer overflow in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9423**	m/blob/master/ChangeLog	211216/235
Denial of Service, Execute Code, Overflow	11-12-2016	6.8	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. The feed_table_tag function in w3m doesn't properly validate the value of table span, which allows remote attackers to cause a denial of service (stack and/or heap buffer overflow) and possibly execute arbitrary code via a crafted HTML page. **REFERENCE: CVE-2016-9422**	https://github.com/tats/w3m/blob/master/ChangeLog	A-W3M-W3M-211216/236
Wolfssl					
Wolfssl wolfSSL is a small, portable, embedded SSL/TLS library targeted for use by embedded systems developers.					
NA	13-12-2016	2.1	The C software implementation of RSA in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover RSA keys by leveraging cache-bank hit differences. **REFERENCE: CVE-2016-7439**	https://wolfssl.com/wolfSSL/Blog/Entries/2016/9/26_wolfSSL_3.9.10_Vulnerability_Fixes.html	A-WOL-WOLFS-211216/237
NA	13-12-2016	2.1	The C software implementation of ECC in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover RSA keys by leveraging cache-bank hit differences.	https://wolfssl.com/wolfSSL/Blog/Entries/2016/9/26_wolfSSL_3.9.10_Vulnerability_Fixes.html	A-WOL-WOLFS-211216/238

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-7438		
X.org					
Xorg- server Xorg is the most popular display server among Linux users.					
Denial of Service	13-12-2016	5	The ProcPutImage function in dix/dispatch.c in X.Org Server (aka xserver and xorg-server) before 1.16.4 allows attackers to cause a denial of service (divide-by-zero and crash) via a zero-height PutImage request. **CVE-2015-3418**	https://cgit.freedesktop.org/xorg/xserver/commit/?id=dc777c346d5d452a53b13b917c45f6a1bad2f20b	A-X.O-XORG--211216/239
Zikula					
Zikula Application Framework Zikula is an OpenSource PHP Application Framework, for your small to enterprise business or personal site.					
Directory Traversal	05-12-2016	7.5	Directory traversal vulnerability in file "jcss.php" in Zikula 1.3.x before 1.3.11 and 1.4.x before 1.4.4 on Windows allows a remote attacker to launch a PHP object injection by uploading a serialized file. **REFERENCE: CVE-2016-9835**	https://github.com/zikula/core/blob/1.3/CHANGELOG-1.3.md	A-ZIK-ZIKUL-211216/240
Application; Operating System (A/OS)					
7-zip/Fedoraproject; Oracle					
7- zip/Fedora/Solaris 7-Zip is a utility program to help you extract compressed files and create your own compressed files in several different formats; Fedora is a Linux based operating system; Solaris is a Unix operating system originally developed by Sun Microsystems.					
Execute Code, Overflow	13-12-2016	9.3	Heap-based buffer overflow in the NArchive::NHfs::CHandler::ExtractZlibFile method in 7zip before 16.00 and p7zip allows remote attackers to execute arbitrary code via a crafted HFS+ image. **REFERENCE: CVE-2016-**	http://www.oracle.com/technetwork/topics/security/bulletinoct2016-3090566.html	A-OS-7Z-7ZIP-211216/241

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			2334		
Canonical;Debian/Gnupg					
Ubuntu Linux/Debian Linux/Gnupg; Libgcrypt Ubuntu is a Debian-based Linux operating system and distribution; Debian is a Unix-like computer operating system and a Linux distribution that is composed entirely of free and open-source software, most of which is under the GNU General Public License, and packaged by a group of individuals known as the Debian project; GNUPG is an open source OpenPGP compatible encryption system; Libgcrypt is a cryptographic library developed as a separated module of GnuPG.					
Gain Information	13-12-2016	5	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits. **REFERENCE: CVE-2016-6313**	https://git.gnupg.org/cgi-bin/gitweb.cgi?p=libgcrypt.git;a=blob_plain;f=NEWS	A-OS-CAN-UBUNT-211216/242
Canonical; Fedoraproject/ Djangoproject					
Ubuntu Linux/Fedora/Django Ubuntu is an open source software platform that runs everywhere from IoT devices, the smartphone, the tablet and the PC to the server and the cloud; Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project; Django is a free and open-source web framework, written in Python, which follows the model-view-template (MVT) architectural pattern.					
NA	09-12-2016	6.8	Django before 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3, when settings.DEBUG is True, allow remote attackers to conduct DNS rebinding attacks by leveraging failure to validate the HTTP Host header against settings.ALLOWED_HOSTS. **REFERENCE: CVE-2016-9014**	https://www.djangoproject.com/weblog/2016/nov/01/security-releases/	A-OS-CAN-UBUNT-211216/243
Canonical; Fedoraproject/Djangoproject					
Ubuntu Linux/Fedora/Django Ubuntu is an open source software platform that runs everywhere from IoT devices, the smart phone, the tablet and the PC to the server and the cloud/ Fedora is an operating system based on the Linux kernel, developed by the community-supported Fedora Project/ Django is a free and open-					

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

source web framework, written in Python, which follows the model-view-template (MVT) architectural pattern.					
NA	09-12-2016	7.5	Django 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3 use a hardcoded password for a temporary database user created when running tests with an Oracle database, which makes it easier for remote attackers to obtain access to the database server by leveraging failure to manually specify a password in the database settings TEST dictionary. **REFERENCE: CVE-2016-9013**	https://www.djangoproject.com/weblog/2016/nov/01/security-releases/	A-OS-CAN-UBUNT-211216/244
Debian/Postgresql					
Debian is an operating system and a distribution of Free Software/ PostgreSQL is a powerful, open source object					
Gain Privileges	09-12-2016	4.6	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) " (double quote), (2) \ (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation. **REFERENCE: CVE-2016-5424**	https://www.postgresql.org/docs/current/static/release-9-5-4.html	A-OS-DEB-DEBIA-211216/245
Denial of Service, Execute Code, ,Gain Information	09-12-2016	6.5	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote authenticated users to cause a denial of	https://www.postgresql.org/docs/current/static/release-9-3-14.html	A-OS-DEB-DEBIA-211216/246

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			service (NULL pointer deReference and server crash), obtain sensitive memory information, or possibly execute arbitrary code via (1) a CASE expression within the test value subexpression of another CASE or (2) inlining of an SQL function that implements the equality operator used for a CASE expression involving values of different types. **REFERENCE: CVE-2016-5423**		
Fedoraproject/X.org					
Fedora/Libx11 Fedora is a Linux based operating system; Xlib (also known as libX11) is an X Window System protocol client library written in the C programming language.					
Gain Privileges	13-12-2016	7.5	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations. **REFERENCE: CVE-2016-7943**	https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=8c29f1607a31dac0911e45a0dd3d74173822b3c9	A-OS-FED-FEDOR-211216/247
Gain Privileges	13-12-2016	7.5	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations. **REFERENCE: CVE-2016-7942**	https://cgit.freedesktop.org/xorg/lib/libX11/commit/?id=8ea762f94f4c942d898fdeb590a1630c83235c17	A-OS-FED-FEDOR-211216/248
Fedora/Libxfixes Fedora is a Linux based operating system.					
Overflow; Gain Privileges	13-12-2016	7.5	Integer overflow in X.org libXfixes before 5.0.3 on 32-bit platforms might allow	https://cgit.freedesktop.org/xorg/lib/libX	A-OS-FED-FEDOR-211216/249

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			remote X servers to gain privileges via a length value of INT_MAX, which triggers the client to stop reading data and get out of sync. **REFERENCE: CVE-2016-7944**	fixes/commit/?id=61c1039ee23a2d1de712843bed3480654d7ef42e	
Fedora/Libxi Fedora is a Linux based operating system.					
Denial of Service	13-12-2016	5	X.org libXi before 1.7.7 allows remote X servers to cause a denial of service (infinite loop) via vectors involving length fields. **REFERENCE: CVE-2016-7946**	https://cgit.freedesktop.org/xorg/lib/libXi/commit/?id=19a9cd607de73947fcfb104682f203ffe4e1f4e5	A-OS-FED-FEDOR-211216/250
Denial of Service, Overflow	13-12-2016	5	Multiple integer overflows in X.org libXi before 1.7.7 allow remote X servers to cause a denial of service (out-of-bounds memory access or infinite loop) via vectors involving length fields. **REFERENCE: CVE-2016-7945**	https://cgit.freedesktop.org/xorg/lib/libXi/commit/?id=19a9cd607de73947fcfb104682f203ffe4e1f4e5	A-OS-FED-FEDOR-211216/251
Fedora/Libxrandr Fedora is a Linux based operating system; libXrandr is the runtime library for the X11 RandR extension.					
NA	13-12-2016	7.5	X.org libXrandr before 1.5.1 allows remote X servers to trigger out-of-bounds write operations by leveraging mishandling of reply data. **REFERENCE: CVE-2016-7948**	https://cgit.freedesktop.org/xorg/lib/libXrandr/commit/?id=a0df3e1c7728205e5c7650b2e6dce684139254a6	A-OS-FED-FEDOR-211216/252
Overflow	13-12-2016	7.5	Multiple integer overflows in X.org libXrandr before 1.5.1 allow remote X servers to trigger out-of-bounds write operations via a crafted response. **REFERENCE: CVE-2016-7947**	https://cgit.freedesktop.org/xorg/lib/libXrandr/commit/?id=a0df3e1c7728205e5c7650b2e6dce684139254a6	A-OS-FED-FEDOR-211216/253

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

NA	13-12-2016	7.5	The XRenderQueryFilters function in X.org libXrender before 0.9.10 allows remote X servers to trigger out-of-bounds write operations via vectors involving filter name lengths. **REFERENCE: CVE-2016-7950**	https://cgit.freedesktop.org/xorg/lib/libXrender/commit/?id=8fad00b0b647ee662ce4737ca15be033b7a21714	A-OS-FED-FEDOR-211216/254
Overflow	13-12-2016	7.5	Multiple buffer overflows in the (1) XvQueryAdaptors and (2) XvQueryEncodings functions in X.org libXrender before 0.9.10 allow remote X servers to trigger out-of-bounds write operations via vectors involving length fields. **REFERENCE: CVE-2016-7949**	https://cgit.freedesktop.org/xorg/lib/libXrender/commit/?id=9362c7ddd1af3b168953d0737877bc52d79c94f4	A-OS-FED-FEDOR-211216/255
Denial of Service	13-12-2016	5	X.org libXtst before 1.2.3 allows remote X servers to cause a denial of service (infinite loop) via a reply in the (1) XRecordStartOfData, (2) XRecordEndOfData, or (3) XRecordClientDied category without a client sequence and with attached data. **REFERENCE: CVE-2016-7952**	https://cgit.freedesktop.org/xorg/lib/libXtst/commit/?id=9556ad67af3129ec4a7a4f4b54a0d59701beeae3	A-OS-FED-FEDOR-211216/256
Overflow	13-12-2016	7.5	Multiple integer overflows in X.org libXtst before 1.2.3 allow remote X servers to trigger out-of-bounds memory access operations by leveraging the lack of range checks. **REFERENCE: CVE-2016-7951**	https://cgit.freedesktop.org/xorg/lib/libXtst/commit/?id=9556ad67af3129ec4a7a4f4b54a0d59701beeae3	A-OS-FED-FEDOR-211216/257
Fedora/Libxv Fedora is a Linux based operating system.					
NA	13-12-2016	7.5	The (1) XvQueryAdaptors and (2) XvQueryEncodings	https://cgit.freedesktop.org	A-OS-FED-FEDOR-

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

			functions in X.org libXv before 1.0.11 allow remote X servers to trigger out-of-bounds memory access operations via vectors involving length specifications in received data. **REFERENCE: CVE-2016-5407**	/xorg/lib/libXv/commit/?id=d9da580b46a28ab497de2e94fdc7b9ff953dab17	211216/258
Fedora/Libxvmc Fedora is a Linux based operating system; libXvMC provides an X Window System client interface to the XVideo-MotionCompensation extension to the X protocol.					
Overflow	13-12-2016	7.5	Buffer underflow in X.org libXvMC before 1.0.10 allows remote X servers to have unspecified impact via an empty string. **REFERENCE: CVE-2016-7953**	https://cgit.freedesktop.org/xorg/lib/libXvMC/commit/?id=2cd95e7da8367cccdcdd5c9b160012d1dec5cbdb	A-OS-FED-FEDOR-211216/259
Imagemagick/Oracle					
Imagemagick/Solaris ImageMagick is a software suite to create, edit, compose, or convert bitmap image/ Solaris is a Unix operating system originally developed by Sun Microsystems.					
Denial of Service, Overflow	13-12-2016	6.8	Buffer overflow in the Get8BIMProperty function in MagickCore/property.c in ImageMagick before 6.9.5-4 and 7.x before 7.0.2-6 allows remote attackers to cause a denial of service (out-of-bounds read, memory leak, and crash) via a crafted image. **REFERENCE: CVE-2016-6491**	https://github.com/ImageMagick/ImageMagick/blob/6.9.5-4/ChangeLog	A-OS-IMA-IMAGE-211216/260
Gain Information	13-12-2016	5	MagickCore/property.c in ImageMagick before 7.0.2-1 allows remote attackers to obtain sensitive memory information via vectors involving the q variable, which triggers an out-of-bounds read.	https://github.com/ImageMagick/ImageMagick/commits/7.0.2-1	A-OS-IMA-IMAGE-211216/261

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			REFERENCE: CVE-2016-5842		
Denial of Service, Execute Code, Overflow	13-12-2016	7.5	Integer overflow in MagickCore/profile.c in ImageMagick before 7.0.2-1 allows remote attackers to cause a denial of service (segmentation fault) or possibly execute arbitrary code via vectors involving the offset variable. **REFERENCE: CVE-2016-5841**	https://github.com/ImageMagick/ImageMagick/commits/7.0.2-1	A- OS-IMA-IMAGE-211216/262
NA	13-12-2016	7.5	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of validation of (1) pixel.red, (2) pixel.green, and (3) pixel.blue. **REFERENCE: CVE-2016-5691**	https://github.com/ImageMagick/ImageMagick/commit/5511ef530576ed18fd636baa3bb4eda3d667665d	A-OS-IMA-IMAGE-211216/263
NA	13-12-2016	7.5	The ReadDCMImage function in DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact via vectors involving the for statement in computing the pixel scaling table. **REFERENCE: CVE-2016-5690**	https://github.com/ImageMagick/ImageMagick/commit/5511ef530576ed18fd636baa3bb4eda3d667665d	A-OS-IMA-IMAGE-211216/264
NA	13-12-2016	7.5	The DCM reader in ImageMagick before 6.9.4-5 and 7.x before 7.0.1-7 allows remote attackers to have unspecified impact by leveraging lack of NULL pointer checks. **REFERENCE: CVE-2016-5689**	https://github.com/ImageMagick/ImageMagick/commit/5511ef530576ed18fd636baa3bb4eda3d667665d	A-OS-IMA-IMAGE-211216/265
Overflow	13-12-2016	6.8	The WPG parser in	https://github	A-OS-IMA-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			ImageMagick before 6.9.4-4 and 7.x before 7.0.1-5, when a memory limit is set, allows remote attackers to have unspecified impact via vectors related to the SetImageExtent return-value check, which trigger (1) a heap-based buffer overflow in the SetPixelIndex function or an invalid write operation in the (2) ScaleCharToQuantum or (3) SetPixelIndex functions. **REFERENCE: CVE-2016-5688**	.com/ImageMagick/ImageMagick/commit/fc43974d34318c834fbf78570ca1a3764ed8c7d7	IMAGE-211216/266
NA	13-12-2016	7.5	The VerticalFilter function in the DDS coder in ImageMagick before 6.9.4-3 and 7.x before 7.0.1-4 allows remote attackers to have unspecified impact via a crafted DDS file, which triggers an out-of-bounds read. **REFERENCE: CVE-2016-5687**	http://www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html	A-OS-IMA-IMAGE-211216/267
Oracle/Pivotal Software					
Solaris/Rabbitmq Solaris is a Unix operating system originally developed by Sun Microsystems/ RabbitMQ is open source message broker software that implements the Advanced Message Queuing Protocol (AMQP).					
Denial of Service	09-12-2016	6.8	The Management plugin in RabbitMQ before 3.6.1 allows remote authenticated users with certain privileges to cause a denial of service (resource consumption) via the (1) lengths_age or (2) lengths_incr parameter. **REFERENCE: CVE-2015-8786**	https://github.com/rabbitmq/rabbitmq-management/issues/97	A-OS-ORA-SOLAR-211216/268
Redhat/Tigervnc					
Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation/Tigervnc Red Hat Enterprise Linux (RHEL) is a Linux distribution developed by Red Hat and targeted toward					

the commercial market/ TigerVNC is VNC server and client software, started as a fork of TightVNC in 2009.					
Denial of Service	14-12-2016	7.5	XRegion in TigerVNC allows remote VNC servers to cause a denial of service (NULL pointer deReference) by leveraging failure to check a malloc return value, a similar issue to CVE-2014-6052. **REFERENCE: CVE-2014-8241**	https://bugzilla.redhat.com/show_bug.cgi?id=1151312	A-OS-RED-ENTER-211216/269
Operating System (OS)					
Cisco					
IOS Cisco Networking Software (IOS, XE, XR, and NX-OS) is the world's most widely deployed networking software.					
NA	13-12-2016	5	A vulnerability in the Zone-Based Firewall feature of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated, remote attacker to pass traffic that should otherwise have been dropped based on the configuration. More Information: CSCuz21015. Known Affected Releases: 15.3(3)M3. Known Fixed Releases: 15.6(2)T0.1 15.6(2.0.1a)T0 15.6(2.19)T 15.6(3)M. **REFERENCE: CVE-2016-9201**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-zbf	O-CIS-IOS-211216/270
Bypass	13-12-2016	5.8	A vulnerability in the implementation of X.509 Version 3 for SSH authentication functionality in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on an affected system. More Information: CSCuv89417. Known	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-xe-x509	O-CIS-IOS-211216/271

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Affected Releases: 15.5(2.25)T. Known Fixed Releases: 15.2(4)E1 15.2(4)E2 15.2(4)E3 15.2(4)EA4 15.2(4.0r)EB 15.2(4.1.27)EB 15.2(4.4.2)EA4 15.2(4.7.1)EC 15.2(4.7.2)EC 15.2(5.1.1)E 15.2(5.5.63)E 15.2(5.5.64)E 15.4(1)IA1.80 15.5(3)M1.1 15.5(3)M2 15.5(3)S1.4 15.5(3)S2 15.6(0.22)S0.12 15.6(1)T0.1 15.6(1)T1 15.6(1.15)T 15.6(1.17)S0.7 15.6(1.17)SP 15.6(1.22.1a)T0 15.6(2)S 15.6(2)SP 16.1(1.24) 16.1.2 16.2(0.247) 16.3(0.11) 3.8(1)E Denali-16.1.2. **REFERENCE: CVE-2016-6474**		
NA	13-12-2016	6.1	A vulnerability in Cisco IOS on Catalyst Switches and Nexus 9300 Series Switches could allow an unauthenticated, adjacent attacker to cause a Layer 2 network storm. More Information: CSCuu69332, CSCux07028. Known Affected Releases: 15.2(3)E. Known Fixed Releases: 12.2(50)SE4 12.2(50)SE5 12.2(50)SQ5 12.2(50)SQ6 12.2(50)SQ7 12.2(52)EY4 12.2(52)SE1 12.2(53)EX 12.2(53)SE 12.2(53)SE1 12.2(53)SE2 12.2(53)SG10 12.2(53)SG11 12.2(53)SG2 12.2(53)SG9 12.2(54)SG1 12.2(55)EX3 12.2(55)SE 12.2(55)SE1 12.2(55)SE10 12.2(55)SE2 12.2(55)SE3 12.2(55)SE4 12.2(55)SE5 12.2(55)SE6 12.2(55)SE7	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios	O-CIS-IOS-211216/272

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			12.2(55)SE8 12.2(55)SE9 12.2(58)EZ 12.2(58)SE1 12.2(58)SE2 12.2(60)EZ 12.2(60)EZ1 12.2(60)EZ2 12.2(60)EZ3 12.2(60)EZ4 12.2(60)EZ5 12.2(60)EZ6 12.2(60)EZ7 12.2(60)EZ8 15.0(1)EY2 15.0(1)SE 15.0(1)SE2 15.0(1)SE3 15.0(2)EA 15.0(2)EB 15.0(2)EC 15.0(2)ED 15.0(2)EH 15.0(2)EJ 15.0(2)EJ1 15.0(2)EK1 15.0(2)EX 15.0(2)EX1 15.0(2)EX3 15.0(2)EX4 15.0(2)EX5 15.0(2)EY 15.0(2)EY1 15.0(2)EY2 15.0(2)EZ 15.0(2)SE 15.0(2)SE1 15.0(2)SE2 15.0(2)SE3 15.0(2)SE4 15.0(2)SE5 15.0(2)SE6 15.0(2)SE7 15.0(2)SE9 15.0(2)SG10 15.0(2)SG3 15.0(2)SG6 15.0(2)SG7 15.0(2)SG8 15.0(2)SG9 15.0(2a)EX5 15.1(2)SG 15.1(2)SG1 15.1(2)SG2 15.1(2)SG3 15.1(2)SG4 15.1(2)SG5 15.1(2)SG6 15.2(1)E 15.2(1)E1 15.2(1)E2 15.2(1)E3 15.2(1)EY 15.2(2)E 15.2(2)E3 15.2(2b)E. **REFERENCE: CVE-2016-6473**		
Ios Xr Cisco Networking Software (IOS, XE, XR, and NX-OS) is the world's most widely deployed networking software.					
NA	13-12-2016	7.2	A vulnerability in Cisco IOS XR Software could allow an authenticated, local attacker to log in to the device with the privileges of the root user. More Information: CSCva38434. Known	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-	O-CIS-IOS X-211216/273

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			Affected Releases: 6.1.1.BASE. **REFERENCE: CVE-2016-9215**	iosxr	
Denial of Service	13-12-2016	5	A vulnerability in the HTTP 2.0 request handling code of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Event Management Service daemon (emsd) to crash, resulting in a denial of service (DoS) condition. More Information: CSCvb14425. Known Affected Releases: 6.1.1.BASE. Known Fixed Releases: 6.1.2.6i.MGBL 6.1.22.9i.MGBL 6.2.1.14i.MGBL. **REFERENCE: CVE-2016-9205**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-xr	O-CIS-IOS X-211216/274
Google					
Android Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices					
Denial of Service	06-12-2016	7.1	The GPS component in Android before 05-12-2016 allows man-in-the-middle attackers to cause a denial of service (GPS signal-acquisition delay) via an incorrect xtra.bin or xtra2.bin file on a spoofed Qualcomm gpsonextra.net or izatcloud.net host, aka internal bug 31470303 and external bug 211602 (and AndroidID-7225554). **REFERENCE: CVE-2016-5341**	http://source.android.com/security/bulletin/01-12-2016.html	O-GOO-ANDRO-211216/275
Gain Information	13-12-2016	4.3	An information disclosure vulnerability in libstagefright in Mediaserver in Android	https://source.android.com/security/bull	O-GOO-ANDRO-211216/276

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Android ID: A-31091777. **REFERENCE: CVE-2016-6722**	etin/2016-11-01.html	
Gain Information	13-12-2016	4.3	An information disclosure vulnerability in libstagefright in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Android ID: A-29422020. **REFERENCE: CVE-2016-6720**	https://android.googlesource.com/platform/frameworks/av/+/7c88b498fda1c2b608a9dd73960a2fd4d7b7e3f7	O-GOO-ANDRO-211216/277
Denial of Service	13-12-2016	7.1	A remote denial of service vulnerability in libvpx in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30593752. **REFERENCE: CVE-2016-**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO-211216/278

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			6712		
Denial of Service	13-12-2016	7.1	A remote denial of service vulnerability in libvpx in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30593765. **REFERENCE: CVE-2016-6711**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO-211216/279
Execute Code, Gain Privileges	13-12-2016	9.3	An elevation of privilege vulnerability in libstagefright in Mediaserver in Android 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-31385713. **REFERENCE: CVE-2016-6706**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO-211216/280
Execute Code, Overflow, Memory Corruption	13-12-2016	9.3	A remote code execution vulnerability in libstagefright in Mediaserver in Android 7.0 before 2016-11-01 could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context	https://android.googlesource.com/platform/frameworks/av/+/3b1c9f692c4d4b7a683c2b358fc89e831a641b88	O-GOO-ANDRO-211216/281

			of the Mediaserver process. Android ID: A-31373622. **REFERENCE: CVE-2016-6699**		
Google;Linux					
Android/Linux Kernel Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices; The Linux kernel is a monolithic Unix-like computer operating system kernel.					
Gain Privileges, Bypass	08-12-2016	9.3	arch/arm64/kernel/sys.c in the Linux kernel before 4.0 allows local users to bypass the "strict page permissions" protection mechanism and modify the system-call table, and consequently gain privileges, by leveraging write access. **REFERENCE: CVE-2015-8967**	http://source.android.com/security/bulletin/01-12-2016.html	O-GOO-ANDRO-211216/282
Intel					
Canyon Bios; Citry Bios; City Bios; Swift Canyon Bios NA					
NA	08-12-2016	6.8	SMM call out in all Intel Branded NUC Kits allows a local privileged user to access the System Management Mode and take full control of the platform. **REFERENCE: CVE-2016-8103**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00057&languageid=en-fr	O-INT-CANYO-211216/283
Joyent					
SmartOs SmartOS is a purpose-built, container-native hypervisor and lightweight container host OS.					
Overflow	14-12-2016	6.9	An exploitable buffer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with native file	http://www.talosintelligence.com/reports/TALOS-2016-0253/	O-JOY-SMART-211216/284

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			systems. An attacker can craft an input that can cause a buffer overflow in the path variable leading to an out of bounds memory access and could result in potential privilege escalation. This vulnerability is distinct from REFERENCE: CVE-2016-9033. **REFERENCE: CVE-2016-9035**		
Overflow	14-12-2016	6.9	An exploitable buffer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with 32-bit file systems. An attacker can craft an input that can cause a buffer overflow in the nm variable leading to an out of bounds memory access and could result in potential privilege escalation. This vulnerability is distinct from REFERENCE: CVE-2016-9032. **REFERENCE: CVE-2016-9034**	http://www.talosintelligence.com/reports/TALOS-2016-0252/	O-JOY-SMART-211216/285
Overflow	14-12-2016	6.9	An exploitable buffer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with native file systems. An attacker can	http://www.talosintelligence.com/reports/TALOS-2016-0251/	O-JOY-SMART-211216/286

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			craft an input that can cause a buffer overflow in the path variable leading to an out of bounds memory access and could result in potential privilege escalation. This vulnerability is distinct from REFERENCE: CVE-2016-9035. **REFERENCE: CVE-2016-9033**		
Overflow	14-12-2016	6.9	An exploitable buffer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with native file systems. An attacker can craft an input that can cause a buffer overflow in the nm variable leading to an out of bounds memory access and could result in potential privilege escalation. This vulnerability is distinct from REFERENCE: CVE-2016-9034. **REFERENCE: CVE-2016-9032**	http://www.talosintelligence.com/reports/TALOS-2016-0250/	O-JOY-SMART-211216/287
Overflow	14-12-2016	6.9	An exploitable integer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with 32-bit file systems. An attacker can craft an input that can cause	http://www.talosintelligence.com/reports/TALOS-2016-0249/	O-JOY-SMART-211216/288

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

			a kernel panic and potentially be leveraged into a full privilege escalation vulnerability. This vulnerability is distinct from REFERENCE: CVE-2016-8733. **REFERENCE: CVE-2016-9031**		
Overflow	14-12-2016	7.2	An exploitable integer overflow exists in the Joyent SmartOS 20161110T013148Z Hyprlofs file system. The vulnerability is present in the Ioctl system call with the command HYPRLOFS_ADD_ENTRIES when dealing with native file systems. An attacker can craft an input that can cause a kernel panic and potentially be leveraged into a full privilege escalation vulnerability. This vulnerability is distinct from REFERENCE: CVE-2016-9031. **REFERENCE: CVE-2016-8733**	http://www.talosintelligence.com/reports/TALOS-2016-0248/	O-JOY-SMART-211216/289
Linux					
Linux Kernel The Linux kernel is a monolithic Unix-like computer operating system kernel.					
Denial of Service	08-12-2016	7.8	The icmp6_send function in net/ipv6/icmp.c in the Linux kernel through 4.8.12 omits a certain check of the dst data structure, which allows remote attackers to cause a denial of service (panic) via a fragmented IPv6 packet. **REFERENCE: CVE-2016-9919**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=79dc7e3f1cd323be4c81aa1a94faa1b3ed987fb2	O-LIN-LINUX-211216/290
Denial of Service, Gain	08-12-2016	9.3	Race condition in the ion_ioctl function in	http://git.kernel.org/cgit/li	O-LIN-LINUX-

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**

Privileges			drivers/staging/android/ion/ion.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) by calling ION_IOC_FREE on two CPUs at the same time. **REFERENCE: CVE-2016-9120**	nux/kernel/git/torvalds/linux.git/commit/?id=9590232bb4f4cc824f3425a6e1349afbe6d6d2b7	211216/291
Denial of Service, Gain Privileges	08-12-2016	7.2	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions. **REFERENCE: CVE-2016-8655**	https://bugzilla.redhat.com/show_bug.cgi?id=1400019	O-LIN-LINUX-211216/292
Gain Privileges	08-12-2016	7.2	arch/arm/kernel/sys_oabi-compat.c in the Linux kernel before 4.4 allows local users to gain privileges via a crafted (1) F_OFD_GETLK, (2) F_OFD_SETLK, or (3) F_OFD_SETLKW command in an fcntl64 system call. **REFERENCE: CVE-2015-8966**	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=76cc404bfdc0d419c720de4daaf2584542734f42	O-LIN-LINUX-211216/293

CV Scoring Scale	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**