National Critical Information Infrastructure Protection Centre

CVE Report

01-15th Aug 2016 **Vol. 03 No. 14**

Vulnerability Type(s)	Publish Date	CVSS	Description	Patch	NCIIPC ID
Application (A)					
Adobe					
Experience Manager *Adobe Experience Manager is an enterprise content management solution that helps simplify the management and delivery of your content and assets.*					
Gain Information	2016-08-09	5	The Backup functionality in Adobe Experience Manager 5.6.1, 6.0, 6.1, and 6.2 allows attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4253**	https://helpx.adobe.com/security/products/experience-manager/apsb16-27.html	A-ADO-EXPER--170816/01
Cross Site Scripting	2016-08-09	4.3	Cross-site scripting (XSS) vulnerability in Adobe Experience Manager 5.6.1, 6.0, 6.1, and 6.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4170**	https://helpx.adobe.com/security/products/experience-manager/apsb16-27.html	A-ADO-EXPER--170816/02
Gain Information	2016-08-09	5	Adobe Experience Manager 6.0, 6.1, and 6.2 allow attackers to obtain sensitive audit log event information via unspecified vectors. **Reference: CVE-2016-4169**	https://helpx.adobe.com/security/products/experience-manager/apsb16-27.html	A-ADO-EXPER--170816/03
Cross Site Scripting	2016-08-09	4.3	Cross-site scripting (XSS) vulnerability in Adobe Experience Manager 5.6.1, 6.0, and 6.1 allows remote attackers to inject arbitrary web script or	https://helpx.adobe.com/security/products/experience-manager/apsb16-27.html	A-ADO-EXPER--170816/04

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

			HTML via unspecified vectors. **Reference: CVE-2016-4168**		
Apache					
Activemq *Apache ActiveMQ is an open source message broker written in Java together with a full Java Message Service (JMS) client.*					
Cross Site Scripting; Gain Information	2016-08-05	3.5	The administration web console in Apache ActiveMQ 5.x before 5.11.4, 5.12.x before 5.12.3, and 5.13.x before 5.13.2 allows remote authenticated users to conduct cross-site scripting (XSS) attacks and consequently obtain sensitive information from a Java memory dump via vectors related to creating a queue. **Reference: CVE-2016-0782**	https://bugzilla.redhat.com/show_bug.cgi?id=1317516	A-APA-ACTIV--170816/05
Openoffice *OpenOffice.org (OOo), commonly known as OpenOffice, is a discontinued open-source office suite, while descendant projects are still being developed.*					
Denial of Service; Execute Code	2016-08-05	6.8	The Impress tool in Apache OpenOffice 4.1.2 and earlier allows remote attackers to cause a denial of service (out-of-bounds read or write) or execute arbitrary code via crafted MetaActions in an (1) ODP or (2) OTP file. **Reference: CVE-2016-1513**	http://www.openoffice.org/security/cves/CVE-2016-1513.html	A-APA-OPENO--170816/06
POI *Apache POI is a popular API that allows programmers to create, modify, and display MS Office files using Java programs.*					

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

NA	2016-08-05	4.3	The XLSX2CSV example in Apache POI before 3.14 allows remote attackers to read arbitrary files via a crafted OpenXML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-5000**	NA	A-APA-POI--170816/07
Atlassian					
Bamboo *Bamboo is a continuous integration and delivery tool that ties automated builds, tests and releases together in a single workflow.*					
Execute Code	2016-08-02	7.5	Atlassian Bamboo before 5.11.4.1 and 5.12.x before 5.12.3.1 does not properly restrict permitted deserialized classes, which allows remote attackers to execute arbitrary code via vectors related to XStream Serialization. **Reference: CVE-2016-5229**	https://jira.atlassian.com/browse/BAM-17736	A-ATL-BAMBO--170816/08
Cisco					
Prime Infrastructure *Cisco Prime Infrastructure offers comprehensive lifecycle management of wired/wireless access, campus, and branch networks, rich visibility into end-user connectivity, and application performance assurance.*					

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	2016-08-07	4.3	Cisco Prime Infrastructure 2.2(2) does not properly restrict use of IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks and unspecified other attacks via a crafted web site, related to a "cross-frame scripting (XFS)" issue, aka Bug ID CSCuw65846, a different vulnerability than CVE-2015-6434. **Reference: CVE-2016-1474**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-cpi	A-CIS-PRIME--170816/09
Telepresence Video Communication Server *The Cisco TelePresence Video Communication Server simplifies session management and control of telepresence conferences.*					
Execute Code	2016-08-07	6.5	The administrative web interface in Cisco TelePresence Video Communication Server Expressway X8.5.2 allows remote authenticated users to execute arbitrary commands via crafted fields, aka Bug ID CSCuv12531. **Reference: CVE-2016-1468**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-vcse	A-CIS-TELEP--170816/10
Unified Communications Manager IM And Presence Service *Cisco Unified Communications Manager Instant Messaging (IM) and Presence Service provides native standards-based dual-protocol enterprise instant messaging and network-based presence as part of Cisco Unified Communications.*					
Denial of Service	2016-08-07	7.8	Cisco Unified Communications Manager IM and Presence Service 9.1(1) SU6, 9.1(1) SU6a, 9.1(1) SU7, 10.5(2) SU2, 10.5(2) SU2a, 11.0(1)	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-ucm	A-CIS-UNIFI--170816/11

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

			SU1, and 11.5(1) allows remote attackers to cause a denial of service (sipd process restart) via crafted headers in a SIP packet, aka Bug ID CSCva39072. **Reference: CVE-2016-1466**		
Dashbuilder Project;Redhat					
Dashbuilder/Jboss Bpm Suite;Jboss Enterprise Brms Platform *Dashbuilder is a full featured web application which allows non-technical users to visually create business dashboards; Red Hat JBoss Enterprise Application Platformis used to build, deploy, and host Java applications and services, quickly and flexibly; Business process management (BPM) and business rules management (BRM) systems help business and IT users collaborate to manage business logic and quickly modify procedures and policies as needed.*					
Execute Code; SQL Injection	2016-08-05	7.5	SQL injection vulnerability in the getStringParameterSQL method in main/java/org/dashbuilder/dataprovider/sql/dialect/DefaultDialect.java in Dashbuilder before 0.6.0.Beta1 allows remote attackers to execute arbitrary SQL commands via a data set lookup filter in the (1) Data Set Authoring or (2) Displayer editor UI. **Reference: CVE-2016-4999**	https://github.com/dashbuilder/dashbuilder/commit/8574899e3b6455547b534f570b2330ff772e524b	A-DAS-DASHB--170816/12
Google					
Chrome *Google Chrome is a freeware web browser developed by Google.*					
Denial of Service	2016-08-07	7.5	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	https://crbug.com/633486	A-GOO-CHROM--170816/13

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-2016-5146		
Bypass	2016-08-07	6.8	Blink, as used in Google Chrome before 52.0.2743.116, does not ensure that a taint property is preserved after a structure-clone operation on an ImageBitmap object derived from a cross-origin image, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code. **Reference: CVE-2016-5145**	https://crbug.com/623406	A-GOO-CHROM--170816/14
Bypass	2016-08-07	7.5	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5143. **Reference: CVE-2016-5144**	http://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html	A-GOO-CHROM--170816/15
Bypass	2016-08-07	7.5	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl	http://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html	A-GOO-CHROM--170816/16

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

			parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5144. **Reference: CVE-2016-5143**		
Denial of Service	2016-08-07	7.5	The Web Cryptography API (aka WebCrypto) implementation in Blink, as used in Google Chrome before 52.0.2743.116, does not properly copy data buffers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code, related to NormalizeAlgorithm.cpp and SubtleCrypto.cpp. **CVE-2016-5142**	http://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html	A-GOO-CHROM--170816/17
NA	2016-08-07	5	Blink, as used in Google Chrome before 52.0.2743.116, allows remote attackers to spoof the address bar via vectors involving a provisional URL for an initially empty document, related to FrameLoader.cpp and ScopedPageLoadDeferrer.cpp. **Reference: CVE-2016-5141**	http://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html	A-GOO-CHROM--170816/18
Denial of Service; Overflow	2016-08-07	7.5	Heap-based buffer overflow in the opj_j2k_read_SQcd_SQcc	http://googlechromereleases.blogspot.com/	A-GOO-CHROM--170816/19

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

			function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data. **Reference: CVE-2016-5140**	2016/08/stable-channel-update-for-desktop.html	
Denial of Service; Overflow	2016-08-07	6.8	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data. **Reference: CVE-2016-5139**	http://googlechromereleases.blogspot.com/2016/08/stable-channel-update-for-desktop.html	A-GOO-CHROM--170816/20
HP					
Release Control *HP Release Control is an enterprise level software product which is a part of HP IT Performance Suite. Contents.*					
Denial of Service; Gain Information	2016-08-07	4	HPE Release Control (RC) 9.13, 9.20, and 9.21 before 9.21.0005 p4 allows remote authenticated users to conduct server-side request forgery (SSRF) attacks, and consequently obtain sensitive information or cause a denial of service, via unspecified vectors.	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05219560	A-HP-RELEA--170816/21

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-2016-4374		
IBM					
Connections Portlets *The IBM Connections Portlets for WebSphere Portal delivers the IBM Connections rich set of social software services for use within a WebSphere Portal environment.*					
NA	2016-08-07	5.8	Open redirect vulnerability in the Connections Portlets component 5.x before 5.0.2 for IBM WebSphere Portal allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **Reference: CVE-2016-2989**	http://www-01.ibm.com/support/docview.wss?uid=swg21986393	A-IBM-CONNE--170816/22
Filenet Workplace *FileNet, a company acquired by IBM, developed software to help enterprises manage their content and business processes.*					
NA	2016-08-07	4.9	Open redirect vulnerability in IBM FileNet Workplace 4.0.2 before 4.0.2.14 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **Reference: CVE-2016-5878**	http://www-01.ibm.com/support/docview.wss?uid=swg21987721	A-IBM-FILEN--170816/23
Filenet Workplace *Workplace is an out-of-the-box web application for accessing many CM features.*					
Cross Site Scripting	2016-08-07	3.5	Cross-site scripting (XSS) vulnerability in IBM FileNet Workplace 4.0.2 allows remote authenticated users to inject arbitrary web script or HTML by uploading a file. **Reference: CVE-2016-3054**	http://www-01.ibm.com/support/docview.wss?uid=swg21987129	A-IBM-FILEN--170816/24

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

General Parallel File System *The General Parallel File System (GPFS) is a high-performance clustered file system developed by IBM.*					
Gain Information	2016-08-07	4	IBM General Parallel File System (GPFS) 3.5 before 3.5.0.29 efix 6 and 4.1.1 before 4.1.1.4 efix 9, when the Spectrum Scale GUI is used with DB2 on Linux, UNIX and Windows, allows remote authenticated users to obtain sensitive information via unspecified vectors, as demonstrated by discovering ADMIN passwords. **Reference: CVE-2016-0361**	http://www-01.ibm.com/support/docview.wss?uid=swg21986595	A-IBM-GENER--170816/25
Information Server Framework; Infosphere Information Governance Catalog; Infosphere Information Server Business Glossary *IBM InfoSphere Information Server provides a unified architecture that works with all types of information integration. Common services, unified parallel processing, and unified metadata are at the core of the server architecture; InfoSphere Information Governance Catalog (formerly known as InfoSphere Business Information Exchange) provides comprehensive information integration capabilities to help you understand and govern your information; IBM InfoSphere Business Glossary provides a platform for creating and managing an enterprise vocabulary and classification system.*					
Cross Site Scripting	2016-08-07	3.5	Cross-site scripting (XSS) vulnerability in IBM Information Server Framework 8.5, Information Server Framework and InfoSphere Information Server Business Glossary 8.7 before FP2, Information Server Framework and InfoSphere Information Server Business Glossary 9.1 before 9.1.2.0, Information Server Framework and InfoSphere Information	http://www-01.ibm.com/support/docview.wss?uid=swg21981766	A-IBM-INFOR--170816/26

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

			Governance Catalog 11.3 before 11.3.1.2, and Information Server Framework and InfoSphere Information Governance Catalog 11.5 before 11.5.0.1 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0280**		
Qradar Security Information And Event Manager *IBM QRadar SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network.*					
Execute Code	2016-08-07	9	IBM Security QRadar SIEM 7.1.x and 7.2.x before 7.2.7 allows remote authenticated users to execute arbitrary OS commands as root via unspecified vectors. **Reference: CVE-2016-2875**	http://www-01.ibm.com/support/docview.wss?uid=swg21988094	A-IBM-QRADA--170816/27
Rational Publishing Engine *IBM Rational Publishing Engine automates document generation from Rational solutions and select third-party tools.*					
Execute Code	2016-08-07	5.5	Unrestricted file upload vulnerability in the Document Builder in IBM Rational Publishing Engine (aka RPENG) 2.0.1 before ifix002 allows remote authenticated users to execute arbitrary code by specifying an unexpected file extension. **Reference: CVE-2016-2914**	http://www-01.ibm.com/support/docview.wss?uid=swg21988263	A-IBM-RATIO--170816/28
Rational Publishing Engine *IBM Rational Publishing Engine automates document generation from Rational solutions and select third-*					

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

party tools.					
Cross Site Scripting	2016-08-07	3.5	Cross-site scripting (XSS) vulnerability in the Document Builder in IBM Rational Publishing Engine (aka RPENG) 2.0.1 before ifix002 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-2912**	http://www-01.ibm.com/support/docview.wss?uid=swg21988263	A-IBM-RATIO--170816/29
Sterling Connect Direct For Unix *IBM Sterling Connect Direct for UNIX links technologies and moves all types of information between networked systems and computers.*					
Gain Information	2016-08-07	2.1	IBM Sterling Connect:Direct for Unix 4.1.0 before 4.1.0.4 iFix073 and 4.2.0 before 4.2.0.4 iFix003 uses default file permissions of 0664, which allows local users to obtain sensitive information via standard filesystem operations. **Reference: CVE-2016-0380**	http://www-01.ibm.com/support/docview.wss?uid=swg21988278	A-IBM-STERL--170816/30
Tivoli Storage Flashcopy Manager For Sql Server;Tivoli Storage Manager For Databases Data Protection For Microsoft Sql Server *IBM Spectrum Protect, formerly Tivoli Storage Manager, is a data protection platform that gives enterprises a single point of control and administration for backup and recovery.*					
Gain Information	2016-08-07	2.1	IBM Tivoli Storage Manager for Databases: Data Protection for Microsoft SQL Server (aka IBM Spectrum Protect for Databases) 6.3 before 6.3.1.7 and 6.4 before 6.4.1.9 and Tivoli Storage FlashCopy Manager for Microsoft SQL Server (aka IBM	http://www-01.ibm.com/support/docview.wss?uid=swg21987333	A-IBM-TIVOL--170816/31

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

			Spectrum Protect Snapshot) 3.1 before 3.1.1.7 and 3.2 before 3.2.1.9 allow local users to discover a cleartext SQL Server password by reading the Task List in the MMC GUI. **Reference: CVE-2016-3059**		
Websphere Application Server *WebSphere Application Server (WAS) is a software product that performs the role of a web application server.*					
Denial of Service	2016-08-07	4.3	IBM WebSphere Application Server (WAS) 7.x before 7.0.0.43, 8.0.0.x before 8.0.0.13, 8.5.0.x before 8.5.5.10, 8.5.0.x and 16.0.0.x Liberty before Liberty Fix Pack 16.0.0.3, and 9.0.0.x before 9.0.0.1 allows remote attackers to cause a denial of service via crafted SIP messages. **Reference: CVE-2016-2960**	http://www-01.ibm.com/support/docview.wss?uid=swg21984796	A-IBM-WEBSP--170816/32
Websphere Portal *IBM WebSphere Portal is a set of software tools that enables companies to build and manage web portals.*					
Cross Site Scripting	2016-08-07	3.5	Cross-site scripting (XSS) vulnerability in IBM WebSphere Portal 6.1.0.x through 6.1.0.6 CF27, 6.1.5.x through 6.1.5.3 CF27, 7.x through 7.0.0.2 CF30, 8.0.0.x through 8.0.0.1 CF21, and 8.5.0 before CF10 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-**	http://www-01.ibm.com/support/docview.wss?uid=swg21986461	A-IBM-WEBSP--170816/33

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

			2925		
Libgd					
Libgd *The GD Graphics Library is a graphics software library by Thomas Boutell and others for dynamically manipulating images.*					
Denial of Service	2016-08-07	5	The gdImageCropThreshold function in gd_crop.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 7.0.9, allows remote attackers to cause a denial of service (application crash) via an invalid color index. **Reference: CVE-2016-6128**	https://bugs.php.net/72494	A-LIB-LIBGD--170816/34
Denial of Service; Overflow	2016-08-07	6.8	Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions. **Reference: CVE-2016-5767**	https://bugs.php.net/bug.php?id=72446	A-LIB-LIBGD--170816/35
Denial of Service; Overflow	2016-08-07	6.8	Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before	https://bugs.php.net/bug.php?id=72339	A-LIB-LIBGD--170816/36

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

			7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image. **Reference: CVE-2016-5766**		
Denial of Service; Overflow; Gain Information	2016-08-07	6.4	gd_xbm.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in certain custom PHP 5.5.x configurations, allows context-dependent attackers to obtain sensitive information from process memory or cause a denial of service (stack-based buffer under-read and application crash) via a long name. **Reference: CVE-2016-5116**	https://github.com/libgd/libgd/issues/211	A-LIB-LIBGD--170816/37
Denial of Service	2016-08-07	6.8	gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function. **Reference: CVE-2013-7456**	https://github.com/php/php-src/commit/7a1aac3343af85b4af4df5f8844946eaa27394ab?w=1	A-LIB-LIBGD--170816/38

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

Microsoft					
Edge *Microsoft Edge (codename "Spartan") is a web browser developed by Microsoft and included in the company's Windows 10operating systems, replacing Internet Explorer as the default web browser on all device classes*					
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability." **Reference: CVE-2016-3296**	https://technet.microsoft.com/library/security/MS16-096	A-MIC-EDGE--170816/39
Edge;Internet Explorer *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes; Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft.*					
Gain Information	2016-08-09	2.6	Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to determine the existence of files via a crafted webpage, aka "Internet Explorer Information Disclosure Vulnerability." **Reference: CVE-2016-3329**	NA	A-MIC-EDGE;--170816/40
Gain Information	2016-08-09	2.6	Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3326. **Reference: CVE-2016-3327**	NA	A-MIC-EDGE;--170816/41
Gain	2016-08-09	2.6	Microsoft Internet	NA	A-MIC-EDGE;-

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

Information			Explorer 9 through 11 and Edge allow remote attackers to obtain sensitive information via a crafted web page, aka "Microsoft Browser Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3327. **Reference: CVE-2016-3326**		-170816/42
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3289. **Reference: CVE-2016-3322**	NA	A-MIC-EDGE;--170816/43
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability." **Reference: CVE-2016-3293**	NA	A-MIC-EDGE;--170816/44
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a	NA	A-MIC-EDGE;--170816/45

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

			different vulnerability than CVE-2016-3322. **Reference: CVE-2016-3289**		
Internet Explorer *Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft.*					
Gain Information	2016-08-09	1.9	Microsoft Internet Explorer 10 and 11 load different files for attempts to open a file:// URL depending on whether the file exists, which allows local users to enumerate files via vectors involving a file:// URL and an HTML5 sandbox iframe, aka "Internet Explorer Information Disclosure Vulnerability." **Reference: CVE-2016-3321**	NA	A-MIC-INTER--170816/46
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288. **Reference: CVE-2016-3290**	https://technet.microsoft.com/library/security/MS16-095	A-MIC-INTER--170816/47
Execute Code; Overflow; Memory Corruption	2016-08-09	7.6	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3290. **Reference: CVE-2016-**	https://technet.microsoft.com/library/security/MS16-095	A-MIC-INTER--170816/48

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

			3288		
Office *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft.*					
Execute Code; Overflow; Memory Corruption	2016-08-09	9.3	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, and 2013 RT SP1 allow remote attackers to execute arbitrary code via a crafted file, aka "Graphics Component Memory Corruption Vulnerability." **Reference: CVE-2016-3318**	https://technet.microsoft.com/library/security/MS16-099	A-MIC-OFFIC--170816/49
Office;Word For Mac;Word Viewer *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Microsoft Word is a word processor developed by Microsoft; Microsoft Office for Mac is a version of the Microsoft Office productivity suite for Mac OS X; Word Reader is an easy-to-use Free Word Reader.*					
Execute Code; Overflow; Memory Corruption	2016-08-09	9.3	Microsoft Office 2007 SP3, 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3313**	https://technet.microsoft.com/library/security/MS16-099	A-MIC-OFFIC--170816/50
Office;Word;Word For Mac;Word Viewer *Microsoft Office is an office suite of applications, servers, and services developed by Microsoft; Microsoft Word is a word processor developed by Microsoft; Microsoft Office for Mac is a version of the Microsoft Office productivity suite for Mac OS X; Word Reader is an easy-to-use Free Word Reader.*					
Execute Code; Overflow; Memory Corruption	2016-08-09	9.3	Microsoft Office 2010 SP2, Word 2007 SP3, Word 2010 SP2, Word for Mac 2011, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted file, aka	https://technet.microsoft.com/library/security/MS16-099	A-MIC-OFFIC--170816/51

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

			"Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3317**		
Onenote;Onenote For Mac *Microsoft OneNote is a computer program for free-form information gathering and multi-user collaboration.*					
Gain Information	2016-08-09	4.3	Microsoft OneNote 2007 SP3, 2010 SP2, 2013 SP1, 2013 RT SP1, 2016, and 2016 for Mac allow remote attackers to obtain sensitive information via a crafted OneNote file, aka "Microsoft OneNote Information Disclosure Vulnerability." **Reference: CVE-2016-3315**	https://technet.microsoft.com/library/security/MS16-099	A-MIC-ONENO--170816/52
Word;Word For Mac *Microsoft Word is a word processor developed by Microsoft; Microsoft Word for Mac is a version of the Microsoft Office productivity suite for Mac OS X.*					
Execute Code; Overflow; Memory Corruption	2016-08-09	9.3	Microsoft Word 2013 SP1, 2013 RT SP1, 2016, and 2016 for Mac allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability." **Reference: CVE-2016-3316**	https://technet.microsoft.com/library/security/MS16-099	A-MIC-WORD;--170816/53
Moxa					
Softcms *SoftCMS is a powerful central management software solution that manages large scale CCTV installations in a single interface.*					
Execute Code; SQL Injection	2016-08-07	7.5	SQL injection vulnerability in Moxa SoftCMS before 1.5 allows remote attackers to execute arbitrary SQL commands via	https://ics-cert.us-cert.gov/advisories/ICSA-16-215-01	A-MOX-SOFTC--170816/54

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

			unspecified fields. **Reference: CVE-2016-5792**		
Mozilla					
Firefox *Mozilla Firefox is a free and open-source web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation.*					
NA	2016-08-04	4.3	Mozilla Firefox before 48.0 does not properly set the LINKABLE and URI_SAFE_FOR_UNTRUSTED_CONTENT flags of about: URLs that are used for error pages, which makes it easier for remote attackers to conduct spoofing attacks via a crafted URL, as demonstrated by misleading text after an about:neterror?d= substring. **Reference: CVE-2016-5268**	http://www.mozilla.org/security/announce/2016/mfsa2016-83.html	A-MOZ-FIREF--170816/55
NA	2016-08-04	4.3	Mozilla Firefox before 48.0 on Android allows remote attackers to spoof the address bar via left-to-right characters in conjunction with a right-to-left character set. **Reference: CVE-2016-5267**	http://www.mozilla.org/security/announce/2016/mfsa2016-82.html	A-MOZ-FIREF--170816/56
NA	2016-08-04	5.8	Mozilla Firefox before 48.0 does not properly restrict drag-and-drop (aka dataTransfer) actions for file: URIs, which allows user-assisted remote attackers to access local files via a crafted web site. **Reference: CVE-2016-**	http://www.mozilla.org/security/announce/2016/mfsa2016-81.html	A-MOZ-FIREF--170816/57

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

			5266		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-04	7.5	Integer overflow in the WebSocketChannel class in the WebSockets subsystem in Mozilla Firefox before 48.0 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted packets that trigger incorrect buffer-resize operations during buffering. **Reference: CVE-2016-5261**	http://www.mozilla.org/security/announce/2016/mfsa2016-75.html	A-MOZ-FIREF--170816/58
Gain Information	2016-08-04	4.3	Mozilla Firefox before 48.0 mishandles changes from 'INPUT type="password"' to 'INPUT type="text"' within a single Session Manager session, which might allow attackers to discover cleartext passwords by reading a session restoration file. **Reference: CVE-2016-5260**	http://www.mozilla.org/security/announce/2016/mfsa2016-74.html	A-MOZ-FIREF--170816/59
Execute Code	2016-08-04	6.8	Use-after-free vulnerability in the js::PreliminaryObjectArray::sweep function in Mozilla Firefox before 48.0 allows remote attackers to execute arbitrary code via crafted JavaScript that is mishandled during incremental garbage collection. **Reference: CVE-2016-5255**	http://www.mozilla.org/security/announce/2016/mfsa2016-71.html	A-MOZ-FIREF--170816/60
NA	2016-08-04	4.7	The Updater in Mozilla	http://www.m	A-MOZ-

			Firefox before 48.0 on Windows allows local users to write to arbitrary files via vectors involving the callback application-path parameter and a hard link. **Reference: CVE-2016-5253**	ozilla.org/security/announce/2016/mfsa2016-69.html	FIREF--170816/61
NA	2016-08-04	4.3	Mozilla Firefox before 48.0 allows remote attackers to spoof the location bar via crafted characters in the media type of a data: URL. **Reference: CVE-2016-5251**	http://www.mozilla.org/security/announce/2016/mfsa2016-66.html	A-MOZ-FIREF--170816/62
Gain Information	2016-08-04	5	Mozilla Firefox before 48.0 allows remote attackers to obtain sensitive information about the previously retrieved page via Resource Timing API calls. **Reference: CVE-2016-5250**	https://bugzilla.mozilla.org/show_bug.cgi?id=1254688	A-MOZ-FIREF--170816/63
Denial of Service; Execute Code; Memory Corruption	2016-08-04	6.8	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 48.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. **Reference: CVE-2016-2835**	https://bugzilla.mozilla.org/show_bug.cgi?id=1280443	A-MOZ-FIREF--170816/64
Firefox;Firefox Esr *Mozilla Firefox is a free and open-source web browser developed by the Mozilla Foundation and its subsidiary, the Mozilla Corporation; Firefox ESR is intended for groups who deploy and maintain the*					

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

desktop environment in large organizations such as schools, governments and businesses.					
Cross Site Scripting; Bypass Gain Information	2016-08-04	4	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allow user-assisted remote attackers to bypass the Same Origin Policy, and conduct Universal XSS (UXSS) attacks or read arbitrary files, by arranging for the presence of a crafted HTML document and a crafted shortcut file in the same local directory. **Reference: CVE-2016-5265**	http://www.mozilla.org/security/announce/2016/mfsa2016-80.html	A-MOZ-FIREF--170816/65
Denial of Service; Execute Code; Memory Corruption	2016-08-04	6.8	Use-after-free vulnerability in the nsNodeUtils::NativeAnonymousChildListChange function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an SVG element that is mishandled during effect application. **Reference: CVE-2016-5264**	http://www.mozilla.org/security/announce/2016/mfsa2016-79.html	A-MOZ-FIREF--170816/66
Execute Code	2016-08-04	6.8	The nsDisplayList::HitTest function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 mishandles rendering display transformation, which allows remote attackers to execute arbitrary code via a crafted web	http://www.mozilla.org/security/announce/2016/mfsa2016-78.html	A-MOZ-FIREF--170816/67

			site that leverages "type confusion." **Reference: CVE-2016-5263**		
Cross Site Scripting	2016-08-04	4.3	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 process JavaScript event-handler attributes of a MARQUEE element within a sandboxed IFRAME element that lacks the sandbox="allow-scripts" attribute value, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site. **Reference: CVE-2016-5262**	http://www.mozilla.org/security/announce/2016/mfsa2016-76.html	A-MOZ-FIREF--170816/68
Execute Code	2016-08-04	6.8	Use-after-free vulnerability in the CanonicalizeXPCOMParticipant function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via a script that closes its own Service Worker within a nested sync event loop. **Reference: CVE-2016-5259**	http://www.mozilla.org/security/announce/2016/mfsa2016-73.html	A-MOZ-FIREF--170816/69
Execute Code	2016-08-04	6.8	Use-after-free vulnerability in the WebRTC socket thread in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code	http://www.mozilla.org/security/announce/2016/mfsa2016-72.html	A-MOZ-FIREF--170816/70

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

			by leveraging incorrect free operations on DTLS objects during the shutdown of a WebRTC session. **Reference: CVE-2016-5258**		
Denial of Service; Execute Code; Memory Corruption	2016-08-04	7.5	Use-after-free vulnerability in the nsXULPopupManager::KeyDown function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) by leveraging keyboard access to use the Alt key during selection of top-level menu items. **Reference: CVE-2016-5254**	http://www.mozilla.org/security/announce/2016/mfsa2016-70.html	A-MOZ-FIREF--170816/71
Exec Code Overflow	2016-08-04	6.8	Stack-based buffer underflow in the mozilla::gfx::BasePoint4d function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via crafted two-dimensional graphics data that is mishandled during clipping-region calculations. **Reference: CVE-2016-5252**	http://www.mozilla.org/security/announce/2016/mfsa2016-67.html	A-MOZ-FIREF--170816/72
Denial of Service	2016-08-04	4.3	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 on Linux make cairo	http://www.mozilla.org/security/announce/2016/mfsa201	A-MOZ-FIREF--170816/73

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

			_cairo_surface_get_extents calls that do not properly interact with libav header allocation in FFmpeg 0.10, which allows remote attackers to cause a denial of service (application crash) via a crafted video. **Reference: CVE-2016-2839**	6-65.html	
Exec Code Overflow	2016-08-04	6.8	Heap-based buffer overflow in the nsBidi::BracketData::AddOpening function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via directional content in an SVG document. **Reference: CVE-2016-2838**	http://www.mozilla.org/security/announce/2016/mfsa2016-64.html	A-MOZ-FIREF--170816/74
Exec Code Overflow Bypass	2016-08-04	6.8	Heap-based buffer overflow in the ClearKey Content Decryption Module (CDM) in the Encrypted Media Extensions (EME) API in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 might allow remote attackers to execute arbitrary code by providing a malformed video and leveraging a Gecko Media Plugin (GMP) sandbox bypass. **Reference: CVE-2016-2837**	http://www.mozilla.org/security/announce/2016/mfsa2016-77.html	A-MOZ-FIREF--170816/75
Denial of Service; Execute	2016-08-04	6.8	Multiple unspecified vulnerabilities in the	https://bugzilla.mozilla.org/s	A-MOZ-FIREF--

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

Code; Overflow; Memory Corruption			browser engine in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to Http2Session::Shutdown and SpdySession31::Shutdown, and other vectors. **Reference: CVE-2016-2836**	how_bug.cgi?id=822081	170816/76
Gain Information	2016-08-04	4.3	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 preserve the network connection used for favicon resource retrieval after the associated browser window is closed, which makes it easier for remote web servers to track users by observing network traffic from multiple IP addresses. **Reference: CVE-2016-2830**	http://www.mozilla.org/security/announce/2016/mfsa2016-63.html	A-MOZ-FIREF--170816/77
Netscape Portable Runtime *In computing, the Netscape Portable Runtime, or NSPR, a platform abstraction library, makes all operating systems it supports appear the same to Mozilla-style web-browsers.*					
Denial of Service; Overflow	2016-08-07	7.5	Multiple integer overflows in io/prprf.c in Mozilla Netscape Portable Runtime (NSPR) before 4.12 allow remote attackers to cause a denial of service (buffer overflow) or possibly have	https://hg.mozilla.org/projects/nspr/rev/96381e3aaae2	A-MOZ-NETSC--170816/78

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

			unspecified other impact via a long string to a PR_*printf function. **Reference: CVE-2016-1951**		
Nofollow Links Project					
Nofollow Links *nofollow is a value that can be assigned to the rel attribute of an HTML a element to instruct some search engines that a hyperlink should not influence the link target's ranking in the search engine's index.*					
Cross Site Scripting	2016-08-02	4.3	Cross-site scripting (XSS) vulnerability in the Nofollow Links plugin before 1.0.11 for WordPress allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-4833**	https://wordpress.org/plugins/nofollow-links/changelog/	A-NOF-NOFOL--170816/79
Openbsd					
Openssh *OpenSSH (also known as OpenBSD Secure Shell) is a suite of security-related network-level utilities based on the Secure Shell(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	2016-08-07	7.8	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string. **Reference: CVE-2016-6515**	https://github.com/openssh/openssh-portable/commit/fcd135c9df440bcd2d5870405ad3311743d78d97	A-OPE-OPENS--170816/80
Openshift					
Origin *OpenShift Origin is the upstream community project that powers OpenShift Online, OpenShift Dedicated, and OpenShift Container Platform. Built around a core of Docker container packaging and Kubernetes container cluster management, Origin is also augmented by application lifecycle management functionality and DevOps tooling. Origin provides a complete open source application container platform.*					

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

Gain Information	2016-08-05	1.9	openshift-node in OpenShift Origin 1.1.6 and earlier improperly stores router credentials as envvars in the pod when the --credentials option is used, which allows local users to obtain sensitive private key information by reading the systemd journal. **Reference: CVE-2015-8945**	https://github.com/openshift/origin/issues/3951	A-OPE-ORIGI--170816/81
PHP					
PHP *PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language.*					
Denial of Service; Execute Code	2016-08-07	7.5	php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object. **Reference: CVE-2016-5773**	https://bugs.php.net/bug.php?id=72434	A-PHP-PHP--170816/82
Denial of Service; Execute Code	2016-08-07	7.5	Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x	https://bugs.php.net/bug.php?id=72340	A-PHP-PHP--170816/83

			before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call. **Reference: CVE-2016-5772**		
Denial of Service; Execute Code	2016-08-07	7.5	spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data. **Reference: CVE-2016-5771**	https://bugs.php.net/bug.php?id=72433	A-PHP-PHP--170816/84
Denial of Service; Overflow	2016-08-07	7.5	Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096. **Reference: CVE-2016-5770**	https://bugs.php.net/bug.php?id=72262	A-PHP-PHP--170816/85
Denial of	2016-08-07	7.5	Multiple integer	https://bugs.p	A-PHP-PHP--

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

Service; Overflow			overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions. **Reference: CVE-2016-5769**	hp.net/bug.php?id=72455	170816/86
Denial of Service; Execute Code	2016-08-07	7.5	Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception. **Reference: CVE-2016-5768**	https://bugs.php.net/bug.php?id=72402	A-PHP-PHP--170816/87
DoS Overflow +Info	2016-08-07	6.4	sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from	https://bugs.php.net/bug.php?id=70755	A-PHP-PHP--170816/88

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

			process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging. **Reference: CVE-2016-5114**		
Denial of Service; Overflow	2016-08-07	7.5	Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument. **Reference: CVE-2016-5096**	https://github.com/php/php-src/commit/abd159cce48f3e34f08e4751c568e09677d5ec9c?w=1	A-PHP-PHP--170816/89
Denial of Service; Overflow	2016-08-07	7.5	Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094. **Reference: CVE-2016-5095**	https://bugs.php.net/bug.php?id=72135	A-PHP-PHP--170816/90

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	2016-08-07	7.5	Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function. **Reference: CVE-2016-5094**	https://github.com/php/php-src/commit/0da8b8b801f9276359262f1ef8274c7812d3dfda?w=1	A-PHP-PHP--170816/91
Denial of Service	2016-08-07	7.5	The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call. **Reference: CVE-2016-5093**	https://github.com/php/php-src/commit/97eff7eb57fc2320c267a949cffd622c38712484?w=1	A-PHP-PHP--170816/92
Execute Code	2016-08-07	7.5	Double free vulnerability in the SplDoublyLinkedList::offsetSet function in ext/spl/spl_dllist.c in PHP 7.x before 7.0.6 allows remote attackers to execute arbitrary code via a crafted index.	https://security-tracker.debian.org/tracker/CVE-2016-3132	A-PHP-PHP--170816/93

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-2016-3132		
Denial of Service; Overflow	2016-08-07	7.5	Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class. **Reference: CVE-2016-3078**	https://security-tracker.debian.org/tracker/CVE-2016-3078	A-PHP-PHP--170816/94
Cross Site Scripting	2016-08-07	4.3	The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function. **Reference: CVE-2015-8935**	https://github.com/php/php-src/commit/996faf964bba1aec06b153b370a7f20d3dd2bb8b?w=1	A-PHP-PHP--170816/95
Pulsesecure					
Odyssey Access Client;Pulse Secure Desktop;Pulse Secure Security;Standalone Pulse Installer Service *Odyssey Access Client 802.1X access clients/supplicants ensure the privacy and integrity of user credentials and network data through their robust authentication and data security for global enterprises and government agencies; Pulse secure is a VPN Software.*					
Gain Privileges	2016-08-02	7.2	An unspecified client-	https://kb.puls	A-PUL-

			side component in Pulse Secure Desktop Client before 5.0r15.1, 5.1rX before 5.1r9.1, and 5.2rX before 5.2r4.1; Installer Service (formerly Juniper Installer Service) and Collaboration (formerly Secure Meeting) before 8.0r15.1, 8.1rX before 8.1r9.1, and 8.2rX before 8.2r4.1; and Odyssey Access Client before 5.6r18 on Windows allows local users to gain administrative privileges via unknown vectors. **Reference: CVE-2016-2408**	esecure.net/articles/Pulse_Security_Advisories/SA40241	ODYSS--170816/96
Qemu					
Qemu *QEMU is a generic and open source machine emulator and virtualizer.*					
Denial of Service	2016-08-02	4.9	The virtqueue_pop function in hw/virtio/virtio.c in QEMU allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by submitting requests without waiting for completion. **Reference: CVE-2016-5403**	https://bugzilla.redhat.com/show_bug.cgi?id=1358359	A-QEM-QEMU--170816/97
Redhat					
Jboss Operations Network *JBoss Operations Network simplifies developing, testing, deploying and monitoring your JBoss solutions and the applications running on it .*					
Execute Code	2016-08-02	9	The server in Red Hat JBoss Operations Network (JON) before 3.3.6 allows remote attackers to execute	https://bugzilla.redhat.com/show_bug.cgi?id=1333618	A-RED-JBOSS--170816/98

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

			arbitrary code via a crafted HTTP request, related to message deserialization. **Reference: CVE-2016-3737**		
Network Satellite *In computing, Red Hat Satellite, an open-source systems-management application, allows system administrators to deploy, manage and monitor Red Hat Enterprise Linux and Solaris hosts.*					
Cross Site Scripting	2016-08-05	4.3	Cross-site scripting (XSS) vulnerability in spacewalk-java in Red Hat Satellite 5.7 allows remote attackers to inject arbitrary web script or HTML via a group name, related to viewing snapshot data. **Reference: CVE-2016-3097**	https://bugzilla.redhat.com/show_bug.cgi?id=1322747	A-RED-NETWO--170816/99
Cross Site Scripting	2016-08-05	4.3	Cross-site scripting (XSS) vulnerability in spacewalk-java in Red Hat Satellite 5.7 allows remote attackers to inject arbitrary web script or HTML via the (1) RHNMD User or (2) Filesystem parameters, related to display of monitoring probes. **Reference: CVE-2016-3080**	https://bugzilla.redhat.com/show_bug.cgi?id=1320942	A-RED-NETWO--170816/100
Openshift *OpenShift is a Kubernetes and Docker powered cloud Platform-as-a-Service (PaaS) developed by Red Hat.*					
Gain Information	2016-08-05	6.8	The API server in Kubernetes, as used in Red Hat OpenShift Enterprise 3.2, in a multi tenant environment allows remote authenticated users with knowledge of other project names to obtain sensitive project and	https://bugzilla.redhat.com/show_bug.cgi?id=1356195	A-RED-OPENS--170816/101

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

			user information via vectors related to the watch-cache list. **Reference: CVE-2016-5392**		
SAP					
Hana *SAP HANA Cloud Platform is an open platform-as-a-service providing unique in-memory database and business application services.*					
Bypass	2016-08-05	7.5	The multi-tenant database container feature in SAP HANA does not properly encrypt communications, which allows remote attackers to bypass intended access restrictions and possibly have unspecified other impact via unknown vectors, aka SAP Security Note 2233550. **Reference: CVE-2016-6150**	NA	A-SAP-HANA--170816/102
Denial of Service; Execute Code	2016-08-05	5	SAP HANA DB 1.00.73.00.389160 allows remote attackers to cause a denial of service (process termination) or execute arbitrary code via vectors related to an IMPORT statement, aka SAP Security Note 2233136. **Reference: CVE-2016-6148**	NA	A-SAP-HANA--170816/103
Gain Information	2016-08-05	5	The SQL interface in SAP HANA provides different error messages for failed login attempts depending on whether the username exists and is locked when the	NA	A-SAP-HANA--170816/104

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

			detailed_error_on_connect option is not supported or is configured as "False," which allows remote attackers to enumerate database users via a series of login attempts, aka SAP Security Note 2216869. **Reference: CVE-2016-6145**		
Bypass	2016-08-05	4.3	The SQL interface in SAP HANA before Revision 102 does not limit the number of login attempts for the SYSTEM user when the password_lock_for_system_user is not supported or is configured as "False," which makes it easier for remote attackers to bypass authentication via a brute force attack, aka SAP Security Note 2216869. **Reference: CVE-2016-6144**	NA	A-SAP-HANA--170816/105
Hana Db *SAP HANA is an in-memory, column-oriented, relational database management system developed and marketed by SAP SE.*					
Gain Information	2016-08-05	2.1	The Extended Application Services (aka XS or XS Engine) in SAP HANA DB 1.00.091.00.1418659308 allows local users to obtain sensitive password information via vectors related to passwords in Web Dispatcher trace files, aka SAP Security Note	NA	A-SAP-HANA --170816/106

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

			2148905. **Reference: CVE-2016-3640**		
Hana Sps09 *SAP HANA SPS 09 provides numerous new functionalities developed by SAP.*					
Gain Information	2016-08-05	2.1	SAP HANA SPS09 1.00.091.00.14186593 allows local users to obtain sensitive information by leveraging the EXPORT statement to export files, aka SAP Security Note 2252941. **Reference: CVE-2016-6149**	NA	A-SAP-HANA --170816/107
Trex *T-REX Software is for the processing and analysis of T-RFLP data.*					
Execute Code	2016-08-05	10	An unspecified interface in SAP TREX 7.10 Revision 63 allows remote attackers to execute arbitrary OS commands with SIDadm privileges via unspecified vectors, aka SAP Security Note 2234226. **Reference: CVE-2016-6147**	NA	A-SAP-TREX--170816/108
NA	2016-08-05	7.6	SAP TREX 7.10 Revision 63 allows remote attackers to write to arbitrary files via vectors related to RFC-Gateway, aka SAP Security Note 2203591. **Reference: CVE-2016-6140**	NA	A-SAP-TREX--170816/109
NA	2016-08-05	7.6	SAP TREX 7.10 Revision 63 allows remote attackers to read arbitrary files via unspecified vectors, aka SAP Security Note	NA	A-SAP-TREX--170816/110

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

			2203591. **Reference: CVE-2016-6139**		
Directory Traversal	2016-08-05	10	Directory traversal vulnerability in SAP TREX 7.10 Revision 63 allows remote attackers to read arbitrary files via unspecified vectors, aka SAP Security Note 2203591. **Reference: CVE-2016-6138**	NA	A-SAP-TREX--170816/111
Siemens					
Sinema Server *SINEMA Server and SNMP OPC Server network management products support you with the main network management tasks in industrial environments.*					
Gain Privileges	2016-08-07	7.2	Siemens SINEMA Server uses weak permissions for the application folder, which allows local users to gain privileges via unspecified vectors. **Reference: CVE-2016-6486**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-321174.pdf	A-SIE-SINEM--170816/112
Sophos					
Mobile Control Eas Proxy *NA*					
NA	2016-08-10	5	Sophos EAS Proxy before 6.2.0 for Sophos Mobile Control, when Lotus Traveler is enabled, allows remote attackers to access arbitrary web-resources from the backend mail system via a request for the resource, aka an Open Reverse Proxy vulnerability. **Reference: CVE-2016-6597**		A-SOP-MOBIL--170816/113
Wireshark					
Wireshark					

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

Wireshark is a network protocol analyzer for Unix and Windows.					
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-wbxml.c in the WBXML dissector in Wireshark 2.x before 2.0.5 does not restrict the recursion depth, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-6513**	http://www.wireshark.org/security/wnpa-sec-2016-49.html	A-WIR-WIRES--170816/114
NA	2016-08-06	4.3	epan/dissectors/packet-wap.c in Wireshark 2.x before 2.0.5 omits an overflow check in the tvb_get_guintvar function, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet, related to the MMSE, WAP, WBXML, and WSP dissectors. **Reference: CVE-2016-6512**	http://www.wireshark.org/security/wnpa-sec-2016-48.html	A-WIR-WIRES--170816/115
Denial of Service	2016-08-06	4.3	epan/proto.c in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (OpenFlow dissector large loop) via a crafted packet. **Reference: CVE-2016-6511**	http://www.wireshark.org/security/wnpa-sec-2016-47.html	A-WIR-WIRES--170816/116
Denial of Service; Overflow	2016-08-06	4.3	Off-by-one error in epan/dissectors/packet-rlc.c in the RLC dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows	http://www.wireshark.org/security/wnpa-sec-2016-46.html	A-WIR-WIRES--170816/117

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

			remote attackers to cause a denial of service (stack-based buffer overflow and application crash) via a crafted packet. **Reference: CVE-2016-6510**		
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-ldss.c in the LDSS dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 mishandles conversations, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-6509**	http://www.wireshark.org/security/wnpa-sec-2016-45.html	A-WIR-WIRES--170816/118
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-rlc.c in the RLC dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 uses an incorrect integer data type, which allows remote attackers to cause a denial of service (large loop) via a crafted packet. **Reference: CVE-2016-6508**	http://www.wireshark.org/security/wnpa-sec-2016-44.html	A-WIR-WIRES--170816/119
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-mmse.c in the MMSE dissector in Wireshark 1.12.x before 1.12.13 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet. **Reference: CVE-2016-6507**	http://www.wireshark.org/security/wnpa-sec-2016-43.html	A-WIR-WIRES--170816/120

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	2016-08-06	4.3	epan/dissectors/packet-wsp.c in the WSP dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet. **Reference: CVE-2016-6506**	http://www.wireshark.org/security/wnpa-sec-2016-42.html	A-WIR-WIRES--170816/121
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-packetbb.c in the PacketBB dissector in Wireshark 1.12.x before 1.12.13 and 2.x before 2.0.5 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted packet. **Reference: CVE-2016-6505**	http://www.wireshark.org/security/wnpa-sec-2016-41.html	A-WIR-WIRES--170816/122
Denial of Service	2016-08-06	4.3	epan/dissectors/packet-ncp2222.inc in the NDS dissector in Wireshark 1.12.x before 1.12.13 does not properly maintain a ptvc data structure, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet. **Reference: CVE-2016-6504**	http://www.wireshark.org/security/wnpa-sec-2016-40.html	A-WIR-WIRES--170816/123
Denial of Service	2016-08-06	4.3	The CORBA IDL dissectors in Wireshark 2.x before 2.0.5 on 64-bit Windows platforms do not properly interact with Visual C++	http://www.wireshark.org/security/wnpa-sec-2016-39.html	A-WIR-WIRES--170816/124

			compiler options, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-6503**		
Denial of Service; Overflow	2016-08-07	4.3	epan/dissectors/packet-wbxml.c in the WBXML dissector in Wireshark 1.12.x before 1.12.12 mishandles offsets, which allows remote attackers to cause a denial of service (integer overflow and infinite loop) via a crafted packet. **Reference: CVE-2016-5359**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12408	A-WIR-WIRES--170816/125
Denial of Service	2016-08-07	4.3	epan/dissectors/packet-pktap.c in the Ethernet dissector in Wireshark 2.x before 2.0.4 mishandles the packet-header data type, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-5358**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12440	A-WIR-WIRES--170816/126
Denial of Service	2016-08-07	4.3	wiretap/netscreen.c in the NetScreen file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file.	https://www.wireshark.org/security/wnpa-sec-2016-36.html	A-WIR-WIRES--170816/127

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-2016-5357		
Denial of Service; Overflow	2016-08-07	4.3	wiretap/cosine.c in the CoSine file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file. **Reference: CVE-2016-5356**	https://www.wireshark.org/security/wnpa-sec-2016-35.html	A-WIR-WIRES--170816/128
Denial of Service	2016-08-07	4.3	wiretap/toshiba.c in the Toshiba file parser in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles sscanf unsigned-integer processing, which allows remote attackers to cause a denial of service (application crash) via a crafted file. **CVE-2016-5355**	https://www.wireshark.org/security/wnpa-sec-2016-34.html	A-WIR-WIRES--170816/129
Denial of Service	2016-08-07	4.3	The USB subsystem in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles class types, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-5354**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12356	A-WIR-WIRES--170816/130
Denial of Service	2016-08-07	4.3	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles the reserved C/T value,	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12191	A-WIR-WIRES--170816/131

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

			which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-5353**		
Denial of Service	2016-08-07	4.3	epan/crypt/airpdcap.c in the IEEE 802.11 dissector in Wireshark 2.x before 2.0.4 mishandles certain length values, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-5352**	https://www.wireshark.org/security/wnpa-sec-2016-31.html	A-WIR-WIRES--170816/132
Denial of Service	2016-08-07	4.3	epan/crypt/airpdcap.c in the IEEE 802.11 dissector in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles the lack of an EAPOL_RSN_KEY, which allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-5351**	https://www.wireshark.org/security/wnpa-sec-2016-30.html	A-WIR-WIRES--170816/133
Denial of Service	2016-08-07	4.3	epan/dissectors/packet-dcerpc-spoolss.c in the SPOOLS component in Wireshark 1.12.x before 1.12.12 and 2.x before 2.0.4 mishandles unexpected offsets, which allows remote attackers to cause a denial of service (infinite loop) via a crafted	https://www.wireshark.org/security/wnpa-sec-2016-29.html	A-WIR-WIRES--170816/134

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

			packet. **Reference: CVE-2016-5350**		
Wordpress					
Wordpress *WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.*					
Cross Site Request Forgery	2016-08-07	6.8	Cross-site request forgery (CSRF) vulnerability in the wp_ajax_wp_compression_test function in wp-admin/includes/ajax-actions.php in WordPress before 4.5 allows remote attackers to hijack the authentication of administrators for requests that change the script compression option. **Reference: CVE-2016-6635**	http://codex.wordpress.org/Version_4.5	A-WOR-WORDP--170816/135
Cross Site Scripting	2016-08-07	4.3	Cross-site scripting (XSS) vulnerability in the network settings page in WordPress before 4.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-6634**	http://codex.wordpress.org/Version_4.5	A-WOR-WORDP--170816/136
Bypass	2016-08-07	5	WordPress before 4.5 does not consider octal and hexadecimal IP address formats when determining an intranet address, which allows remote attackers to bypass an intended SSRF protection mechanism via a crafted address. **Reference: CVE-2016-4029**	http://codex.wordpress.org/Version_4.5	A-WOR-WORDP--170816/137

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

Application; Operating System (A/OS)

Canonical/KDE					
Ubuntu Linux/Karchives *Ubuntu is an open source software platform that runs everywhere from the smartphone, the tablet and the PC to the server and the cloud.*					
Directory Traversal	2016-08-02	5	Directory traversal vulnerability in KArchive before 5.24, as used in KDE Frameworks, allows remote attackers to write to arbitrary files via a ../ (dot dot slash) in a filename in an archive file, related to KNewsstuff downloads. **Reference: CVE-2016-6232**	https://www.kde.org/info/security/advisory-20160724-1.txt	A-OS-CAN-UBUNT--170816/138
Debian/Djangoproject					
Debian Linux/Django *Debian is an operating system and a distribution of Free Software; Django is a free and open-source web framework, written in Python, which follows the model–view–controller (MVC) architectural pattern.*					
Cross Site Scripting	2016-08-05	4.3	Cross-site scripting (XSS) vulnerability in the dismissChangeRelatedObjectPopup function in contrib/admin/static/admin/js/admin/RelatedObjectLookups.js in Django before 1.8.14, 1.9.x before 1.9.8, and 1.10.x before 1.10rc1 allows remote attackers to inject arbitrary web script or HTML via vectors involving unsafe usage of Element.innerHTML. **Reference: CVE-2016-6186**	https://www.djangoproject.com/weblog/2016/jul/18/security-releases/	A-OS-DEB-DEBIA--170816/139
Debian/Haxx					
Debian Linux/Libcurl *Debian is an operating system and a distribution of Free Software; libcurl is a free and easy-to-use client-side URL transfer library, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP.*					
NA	2016-08-10	7.5	Use-after-free		A-OS-DEB-

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

			vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors. **Reference: CVE-2016-5421**		DEBIA--170816/140
NA	2016-08-10	5	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate. **Reference: CVE-2016-5420**		A-OS-DEB-DEBIA--170816/141
Bypass	2016-08-10	5	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session. **Reference: CVE-2016-5419**		A-OS-DEB-DEBIA--170816/142
Debian/Libgd					
Debian Linux/Libgd *Debian is an operating system and a distribution of Free Software; GD is an open source code library for the dynamic creation of images by programmers.*					
Denial of Service	2016-08-12	4.3	gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds	https://libgd.github.io/release-2.2.3.html	A-OS-DEB-DEBIA--170816/143

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

			read) via a crafted TGA file. **Reference: CVE-2016-6214**		
Denial of Service; Overflow	2016-08-12	4.3	Integer overflow in the _gdContributionsAlloc function in gd_interpolation.c in GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds memory write or memory consumption) via unspecified vectors. **Reference: CVE-2016-6207**	https://libgd.github.io/release-2.2.3.html	A-OS-DEB-DEBIA--170816/144
Denial of Service	2016-08-12	4.3	The output function in gd_gif_out.c in the GD Graphics Library (aka libgd) allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image. **Reference: CVE-2016-6161**	https://github.com/libgd/libgd/issues/209	A-OS-DEB-DEBIA--170816/145
Denial of Service	2016-08-12	4.3	The gdImageCreateFromTgaCtx function in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file. **Reference: CVE-2016-6132**	https://libgd.github.io/release-2.2.3.html	A-OS-DEB-DEBIA--170816/146
Debian/Perl					
Debian Linux/Perl *Debian is an operating system and a distribution of Free Software/Perl is a family of high-level, general-purpose, interpreted, dynamic programming languages.*					
Gain Privileges	2016-08-02	7.2	(1) cpan/Archive-	https://rt.perl.	A-OS-DEB-

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

		🟧	Tar/bin/ptar, (2) cpan/Archive-Tar/bin/ptardiff, (3) cpan/Archive-Tar/bin/ptargrep, (4) cpan/CPAN/scripts/cpan, (5) cpan/Digest-SHA/shasum, (6) cpan/Encode/bin/enc2xs, (7) cpan/Encode/bin/encguess, (8) cpan/Encode/bin/piconv, (9) cpan/Encode/bin/ucmlint, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instmodsh, (12) cpan/IO-Compress/bin/zipdetails, (13) cpan/JSON-PP/bin/json_pp, (14) cpan/Test-Harness/bin/prove, (15) dist/ExtUtils-ParseXS/lib/ExtUtils/xsubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) utils/c2ph.PL, (19) utils/h2ph.PL, (20) utils/h2xs.PL, (21) utils/libnetcfg.PL, (22) utils/perlbug.PL, (23) utils/perldoc.PL, (24) utils/perlivp.PL, and (25) utils/splain.PL in Perl 5.x before 5.22.3-RC2 and 5.24 before 5.24.1-RC2 do not properly remove . (period) characters from the end of the includes	org/Public/Bug/Display.html?id=127834	DEBIA--170816/147

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

			directory array, which might allow local users to gain privileges via a Trojan horse module under the current working directory. **Reference: CVE-2016-1238**		
Debian/Pivotal Software					
Debian Linux/Redis *Red Hat Enterprise Linux (RHEL) is a Linux distribution developed by Red Hat and targeted toward the commercial market.*					
Gain Information	2016-08-10	2.1	linenoise, as used in Redis before 3.2.3, uses world-readable permissions for .rediscli_history, which allows local users to obtain sensitive information by reading the file. **Reference: CVE-2013-7458**	https://github.com/antirez/redis/pull/1418	A-OS-DEB-DEBIA--170816/148
Debian;Fedoraproject/Perl					
Debian Linux/Fedora/Perl *Debian is an operating system and a distribution of Free Software/Fedora is an operating system based on the Linux kernel, developed by the community-supported Fedora Project/Perl is a family of high-level, general-purpose, interpreted, dynamic programming languages.*					
Execute Code	2016-08-02	4.6	The XSLoader::load method in XSLoader in Perl does not properly locate .so files when called in a string eval, which might allow local users to execute arbitrary code via a Trojan horse library under the current working directory. **Reference: CVE-2016-6185**	https://rt.cpan.org/Public/Bug/Display.html?id=115808	A-OS-DEB-DEBIA--170816/149
IBM/IBM					
AIX;Vios/Vios *AIX is an open operating system from IBM that is based on a version of UNIX; VIOS (Virtual I/O Server) is a IBM virtualization software product.*					

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	2016-08-07	4.3	The mustendd driver in IBM AIX 5.3, 6.1, 7.1, and 7.2 and VIOS 2.2.x, when the jumbo_frames feature is not enabled, allows remote attackers to cause a denial of service (FC1763 or FC5899 adapter crash) via crafted packets. **Reference: CVE-2016-0281**	http://aix.software.ibm.com/aix/efixes/security/mustendd_advisory.asc	A-OS-IBM-AIX;V--170816/150
Vmware/Vmware					
Esxi/Fusion;Tools; Workstation Player; Workstation Pro *VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers; VMware Workstation 12 Player is a desktop virtualization application that runs one or more operating systems on the same computer without rebooting; VMware Workstation Pro is the easiest to use, the fastest and the most reliable app when it comes to evaluating a new OS, or new software apps and patches, in an isolated and safe virtualized environment.*					
Gain Privileges	2016-08-07	4.4	Untrusted search path vulnerability in the HGFS (aka Shared Folders) feature in VMware Tools 10.0.5 in VMware ESXi 5.0 through 6.0, VMware Workstation Pro 12.1.x before 12.1.1, VMware Workstation Player 12.1.x before 12.1.1, and VMware Fusion 8.1.x before 8.1.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory. **Reference: CVE-2016-5330**	http://www.vmware.com/security/advisories/VMSA-2016-0010.html	A-OS-VMW-ESXI/--170816/151
Esxi/Vcenter Server *VMware ESXi (formerly ESX) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers/ vCenter server is installed on Windows Server or Linux Server. VMware vCenter server is a centralized management application that lets you manage virtual machines and ESXi hosts centrally. vSphere client is used to access vCenter Server and ultimately manage ESXi servers.*					
Http R.Spl.	2016-08-07	4.3	CRLF injection vulnerability in VMware vCenter Server 6.0	http://www.vmware.com/security/advisori	A-OS-VMW-ESXI/--170816/152

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

			before U2 and ESXi 6.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. **Reference: CVE-2016-5331**	es/VMSA-2016-0010.html	
Citrix/XEN					
Xenserver/XEN *XenServer is the leading open source virtualization platform, powered by the Xen hypervisor; Xen Project is a hypervisor using a microkernel design, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently.*					
Denial of Service	2016-08-02	4.9	Xen 4.5.x through 4.7.x do not implement Supervisor Mode Access Prevention (SMAP) whitelisting in 32-bit exception and event delivery, which allows local 32-bit PV guest OS kernels to cause a denial of service (hypervisor and VM crash) by triggering a safety check. **Reference: CVE-2016-6259**	http://xenbits.xen.org/xsa/xsa183-unstable.patch	A-OS-CIT-XENSE--170816/153
Gain Privileges	2016-08-02	7.2	The PV pagetable code in arch/x86/mm.c in Xen 4.7.x and earlier allows local 32-bit PV guest OS administrators to gain host OS privileges by leveraging fast-paths for updating pagetable entries. **Reference: CVE-2016-6258**	http://xenbits.xen.org/xsa/xsa182-unstable.patch	A- OS-CIT-XENSE--170816/154
Microsoft/Microsoft					
Edge/Windows 10;Windows 8.1;Windows Server 2012 *Microsoft Edge is a web browser developed by Microsoft and included in the company's Windows 10 operating systems, replacing Internet Explorer as the default web browser on all device classes;Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows Server is a brand name for a group of server operating systems released by*					

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

Microsoft.					
Execute Code	2016-08-09	9.3	The PDF library in Microsoft Windows 8.1; Windows Server 2012 Gold and R2; Windows 10 Gold, 1511, and 1607; and Microsoft Edge allows remote attackers to execute arbitrary code via a crafted PDF file, aka "Microsoft PDF Remote Code Execution Vulnerability." **Reference: CVE-2016-3319**		A- OS-MIC-EDGE/--170816/155
Live Meeting;Lync;Office;Skype For Business;Word Viewer/Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Vista *Microsoft Office Live Meeting is a discontinued commercial subscription-based web conferencing service operated by Microsoft.Skype for Business (formerly Microsoft Office Communicator and Microsoft Lync) and Microsoft Lync for Mac are instant-messaging clients used with Skype for Business Server or with Lync Online (available with Microsoft Office 365); Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft; Windows Vista is an operating system by Microsoft for use on personal computers, including home and business desktops, laptops, tablet PCs, and media center PCs; After installing Word Viewer you can open and view DOC files without having to use Microsoft Office Word.*					
Execute Code	2016-08-09	9.3	The Windows font library in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; Windows 10 Gold, 1511, and 1607; Office 2007 SP3; Office 2010 SP2; Word Viewer; Skype for Business 2016; Lync 2013 SP1; Lync 2010; Lync 2010 Attendee; and Live Meeting 2007 Console allows remote attackers to execute	http://technet.microsoft.com/en-us/security/bulletin/ms16-097	A- OS-MIC-LIVE --170816/156

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

			arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability." **Reference: CVE-2016-3301**		
Live Meeting; Lync; Office; Skype For Business; Word Viewer/Windows 7;Windows Server 2008;Windows Vista *Microsoft Office Live Meeting is a discontinued commercial subscription-based web conferencing service operated by Microsoft.Skype for Business (formerly Microsoft Office Communicator and Microsoft Lync) and Microsoft Lync for Mac are instant-messaging clients used with Skype for Business Server or with Lync Online (available with Microsoft Office 365); Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft; Windows Vista is an operating system by Microsoft for use on personal computers, including home and business desktops, laptops, tablet PCs, and media center PCs; After installing Word Viewer you can open and view DOC files without having to use Microsoft Office Word.*					
Execute Code	2016-08-09	9.3	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability," a different vulnerability than CVE-2016-3303. **Reference: CVE-2016-3304**	http://technet.microsoft.com/en-us/security/bulletin/ms16-097	A- OS-MIC-LIVE --170816/157
Execute Code	2016-08-09	9.3	The Windows font library in Microsoft Windows Vista SP2,	http://technet.microsoft.com/en-	A-OS-MIC-LIVE --170816/158

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

		🟥	Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee, and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability," a different vulnerability than CVE-2016-3304. **Reference: CVE-2016-3303**	us/security/bulletin/ms16-097	
Hardware/ Operating System (H/OS)					
Amazonbasics; Dell; Lenovo; Logitech/Dell					
NA	2016-08-02	3.3	The firmware in Lenovo Ultraslim dongles, as used with Lenovo Liteon SK-8861, Ultraslim Wireless, and Silver Silk keyboards and Liteon ZTM600 and Ultraslim Wireless mice, does not enforce incrementing AES counters, which allows remote attackers to inject encrypted keyboard input into the system by leveraging proximity to the dongle, aka a "KeyJack injection attack." **Reference: CVE-2016-6257**	https://support.lenovo.com/product_security/len_7267	H-OS-AMA-FIRMW--170816/159
Operating System (OS)					
Cisco					
IOS					

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

iOS (originally iPhone OS) is a mobile operating system created and developed by Apple Inc. and distributed exclusively for Apple hardware.					
Denial of Service	2016-08-07	7.8	Cisco IOS 15.5(3)S3, 15.6(1)S2, 15.6(2)S1, and 15.6(2)T1 does not properly dequeue invalid NTP packets, which allows remote attackers to cause a denial of service (interface wedge) by sending many crafted NTP packets, aka Bug ID CSCva35619. **Reference: CVE-2016-1478**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160804-wedge	O-CIS-IOS--170816/160
Rv110w Wireless-n Vpn Firewall Firmware;Rv130w Wireless-n Multifunction Vpn Router Firmware;Rv215w Wireless-n Vpn Router Firmware *Cisco Small Business RV Series Routers offer virtual private networking (VPN) technology that lets your remote workers connect to your network through a secure Internet pathway.*					
NA	2016-08-07	9	Cisco RV110W, RV130W, and RV215W devices have an incorrect RBAC configuration for the default account, which allows remote authenticated users to obtain root access via a login session with that account, aka Bug IDs CSCuv90139, CSCux58175, and CSCux73557. **Reference: CVE-2015-6397**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv110_130w2	O-CIS-RV110--170816/161
Execute Code	2016-08-07	7.2	The CLI command parser on Cisco RV110W, RV130W, and RV215W devices allows local users to execute arbitrary shell commands as an administrator via crafted parameters, aka Bug IDs	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv110_130w1	O-CIS-RV110--170816/162

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

			CSCuv90134, CSCux58161, and CSCux73567. **Reference: CVE-2015-6396**		
Rv180 Vpn Router Firmware;Rv180w Vpn Router Firmware *The Cisco RV180 VPN Router delivers highly secure broadband connectivity and remote access for multiple offices and remote workers.*					
Execute Code	2016-08-07	9	Cisco RV180 and RV180W devices allow remote authenticated users to execute arbitrary commands as root via a crafted HTTP request, aka Bug ID CSCuz48592. **Reference: CVE-2016-1430**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv180_2	O-CIS-RV180--170816/163
Rv180 Vpn Router Firmware;Rv180w Wireless-n Multifunction Vpn Router Firmware *The Cisco RV180 VPN Router delivers highly secure broadband connectivity and remote access for multiple offices and remote workers.*					
Directory Traversal	2016-08-07	7.8	Directory traversal vulnerability in the web interface on Cisco RV180 and RV180W devices allows remote attackers to read arbitrary files via a crafted HTTP request, aka Bug ID CSCuz43023. **Reference: CVE-2016-1429**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160803-rv180_1	O-CIS-RV180--170816/164
Crestron					
Airmedia Am-100 Firmware *The AirMedia (AM-100) is a device which allows users to present their HD content to projectors and displays using the existing IT infrastructure, without the hassle of connecting wires.*					
Execute Code; Directory Traversal	2016-08-02	10	Directory traversal vulnerability in cgi-bin/rftest.cgi on Crestron AirMedia AM-100 devices with firmware before 1.4.0.13 allows remote attackers to execute arbitrary commands via a .. (dot dot) in the		O-CRE-AIRME--170816/165

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

			ATE_COMMAND parameter. **Reference: CVE-2016-5640**		
Directory Traversal	2016-08-02	5	Directory traversal vulnerability in cgi-bin/login.cgi on Crestron AirMedia AM-100 devices with firmware before 1.4.0.13 allows remote attackers to read arbitrary files via a .. (dot dot) in the src parameter. **Reference: CVE-2016-5639**		O-CRE-AIRME--170816/166
Dm-txrx-100-str Firmware *The Crestron DM-TXRX-100-STR is a compact H.264 streaming encoder/decoder designed to enable the distribution of high-definition AV signals over an IP network.*					
Cross Site Request Forgery	2016-08-02	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities on Crestron Electronics DM-TXRX-100-STR devices with firmware through 1.3039.00040 allow remote attackers to hijack the authentication of arbitrary users. **Reference: CVE-2016-5671**	NA	O-CRE-DM-TX--170816/167
NA	2016-08-02	10	Crestron Electronics DM-TXRX-100-STR devices with firmware before 1.3039.00040 have a hardcoded password of admin for the admin account, which makes it easier for remote attackers to obtain access via the web management interface. **Reference: CVE-2016-**	NA	O-CRE-DM-TX--170816/168

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

		🟥	**5670**		
NA	2016-08-02	5	Crestron Electronics DM-TXRX-100-STR devices with firmware before 1.3039.00040 use a hardcoded 0xb9eed4d955a59eb3 X.509 certificate from an OpenSSL Test Certification Authority, which makes it easier for remote attackers to conduct man-in-the-middle attacks against HTTPS sessions by leveraging the certificate's trust relationship. **Reference: CVE-2016-5669**	NA	O-CRE-DM-TX--170816/169
Bypass	2016-08-02	7.5	Crestron Electronics DM-TXRX-100-STR devices with firmware before 1.3039.00040 allow remote attackers to bypass authentication and change settings via a JSON API call. **Reference: CVE-2016-5668**	NA	O-CRE-DM-TX--170816/170
Bypass	2016-08-02	7.5	Crestron Electronics DM-TXRX-100-STR devices with firmware before 1.3039.00040 allow remote attackers to bypass authentication via a direct request to a page other than index.html. **Reference: CVE-2016-5667**	NA	O-CRE-DM-TX--170816/171
NA	2016-08-02	5	Crestron Electronics DM-TXRX-100-STR devices with firmware before 1.3039.00040	NA	O-CRE-DM-TX--170816/172

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

			rely on the client to perform authentication, which allows remote attackers to obtain access by setting the value of objresp.authenabled to 1. **Reference: CVE-2016-5666**		
Debian;Linux					
Debian Linux/Linux Kernel *Debian is an operating system and a distribution of Free Software/ The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service	2016-08-06	4.6	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by triggering a certain page move. **Reference: CVE-2016-3070**	https://github.com/torvalds/linux/commit/42cb14b110a5698ccf26ce59c4441722605a3743	O-DEB-DEBIA--170816/173
Fortinet					
Fortianalyzer Firmware;Fortimanager Firmware *Fortinet is an American multinational corporation headquartered in Sunnyvale, California. It develops and markets cybersecurity software, appliances and services, such as firewalls, anti-virus, intrusion prevention and endpoint security, among others. It is the fourth-largest network security company by revenue.*					
Cross Site Scripting	2016-08-05	3.5	Cross-site scripting (XSS) vulnerability in Fortinet FortiAnalyzer 5.x before 5.2.6 and FortiManager 5.x before 5.2.6 allows remote authenticated users to inject arbitrary web	http://fortiguard.com/advisory/fortimanager-and-fortianalyzer-persistent-xss-vulnerability	O-FOR-FORTI--170816/174

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

			script or HTML via the filename of an image uploaded in the report section. **Reference: CVE-2016-3196**		
Google					
Android *Android (from its former owner Android, Inc.) is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touch-screen mobile devices such as smartphones and tablets.*					
Gain Privileges	2016-08-05	9.3	The kernel in Android before 2016-08-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka internal bug 28522518. **Reference: CVE-2016-3857**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/175
Bypass	2016-08-05	4.9	Google Play services in Android before 2016-08-05 on Nexus devices allow local users to bypass the Factory Reset Protection protection mechanism and delete data via unspecified vectors, aka internal bug 26803208. **Reference: CVE-2016-3853**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/176
Gain Information	2016-08-05	4.3	The MediaTek Wi-Fi driver in Android before 2016-08-05 on Android One devices allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 29141147 and MediaTek internal bug ALPS02751738. **Reference: CVE-2016-3852**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/177

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

Gain Privileges	2016-08-05	9.3	The LG Electronics bootloader Android before 2016-08-05 on Nexus 5X devices allows attackers to gain privileges by leveraging access to a privileged process, aka internal bug 29189941. **Reference: CVE-2016-3851**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/178
Overflow; Gain Privileges	2016-08-05	6.9	Integer overflow in app/aboot/aboot.c in the Qualcomm bootloader in Android before 2016-08-05 on Nexus 5, 5X, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted header field in a boot image, aka Android internal bug 27917291 and Qualcomm internal bug CR945164. **Reference: CVE-2016-3850**	https://source.codeaurora.org/quic/la/kernel/lk/commit/?id=030371d45a9dcda4d0cc3c76647e753a1cc1b782	O-GOO-ANDRO--170816/179
Gain Privileges	2016-08-05	6.9	The ION driver in Android before 2016-08-05 on Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28939740. **Reference: CVE-2016-3849**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/180
Gain Privileges	2016-08-05	7.6	The NVIDIA media driver in Android before 2016-08-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28919417. **Reference: CVE-2016-3848**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/181

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

Gain Privileges	2016-08-05	6.9	The NVIDIA media driver in Android before 2016-08-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application, aka internal bug 28871433. **Reference: CVE-2016-3847**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/182
Gain Privileges	2016-08-05	7.6	The Serial Peripheral Interface driver in Android before 2016-08-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application, aka internal bug 28817378. **Reference: CVE-2016-3846**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/183
Gain Privileges	2016-08-05	9.3	The video driver in the kernel in Android before 2016-08-05 on Nexus 5 devices allows attackers to gain privileges via a crafted application, aka internal bug 28399876. **Reference: CVE-2016-3845**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/184
Gain Privileges	2016-08-05	9.3	mediaserver in Android before 2016-08-05 on Nexus 9 and Pixel C devices allows attackers to gain privileges via a crafted application, aka internal bug 28299517. **Reference: CVE-2016-3844**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/185
Execute Code; Gain Privileges	2016-08-05	9.3	Android before 2016-08-05 does not properly restrict code execution in a kernel context, which allows attackers to gain privileges via a crafted application, as	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/186

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

			demonstrated by the kernel performance subsystem and the Qualcomm performance component, aka Android internal bugs 28086229 and 29119870 and Qualcomm internal bug CR1011071. **Reference: CVE-2016-3843**		
Gain Privileges	2016-08-05	9.3	The Qualcomm GPU driver in Android before 2016-08-05 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28377352 and Qualcomm internal bug CR1002974. **Reference: CVE-2016-3842**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/187
Execute Code	2016-08-05	10	Conscrypt 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 2016-08-05 does not properly identify session reuse, which allows remote attackers to execute arbitrary code via unspecified vectors, aka internal bug 28751153. **Reference: CVE-2016-3840**	https://android.googlesource.com/platform/external/conscrypt/+/5af5e93463f4333187e7e35f3bd2b846654aa214	O-GOO-ANDRO--170816/188
Denial of Service	2016-08-05	4.3	Bluetooth 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 2016-08-01 allows attackers to cause a denial of service (loss of Bluetooth 911 functionality) via a crafted application that	https://android.googlesource.com/platform/system/bt/+/472271b153c5dc53c28beac55480a8d8434b2d5c	O-GOO-ANDRO--170816/189

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

			sends a signal to a Bluetooth process, aka internal bug 28885210. **Reference: CVE-2016-3839**		
Denial of Service	2016-08-05	4.3	Android 6.x before 2016-08-01 allows attackers to cause a denial of service (loss of locked-screen 911 functionality) via a crafted application that uses the app-pinning feature, aka internal bug 28761672. **Reference: CVE-2016-3838**	https://android.googlesource.com/platform/frameworks/base/+/468651c86a8adb7aa56c708d2348e99022088af3	O-GOO-ANDRO--170816/190
Gain Information	2016-08-05	4.3	service/jni/com_android_server_wifi_WifiNative.cpp in Wi-Fi in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allows attackers to obtain sensitive information via a crafted application that provides a MAC address with too few characters, aka internal bug 28164077. **Reference: CVE-2016-3837**	https://android.googlesource.com/platform/frameworks/opt/net/wifi/+/a209ff12ba9617c10550678ff93d01fb72a33399	O-GOO-ANDRO--170816/191
Gain Information	2016-08-05	4.3	The SurfaceFlinger service in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allows attackers to obtain sensitive information via a crafted application, related to lack of a default constructor in include/ui/FrameStats.h, aka internal bug 28592402.	https://android.googlesource.com/platform/frameworks/native/+/3bcf0caa8cca9143443814b36676b3bae33a4368	O-GOO-ANDRO--170816/192

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-2016-3836		
Gain Information	2016-08-05	4.3	The secure-session feature in the mm-video-v4l2 venc component 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 2016-08-01 mishandles heap pointers, which allows attackers to obtain sensitive information via a crafted application, aka internal bug 28920116. **Reference: CVE-2016-3835**	https://android.googlesource.com/platform/hardware/qcom/media/+/7558d03e6498e970b761aa44fff6b2c659202d95	O-GOO-ANDRO--170816/193
Bypass; Gain Information	2016-08-05	4.3	The camera APIs 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 2016-08-01 allow attackers to bypass intended access restrictions and obtain sensitive information about ANW buffer addresses via a crafted application, aka internal bug 28466701. **Reference: CVE-2016-3834**	https://android.googlesource.com/platform/frameworks/av/+/1f24c730ab6ca5aff1e3137b340b8aeaeda4bdbc	O-GOO-ANDRO--170816/194
Bypass	2016-08-05	9.3	The Shell component in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 does not properly manage the MANAGE_USERS and CREATE_USERS permissions, which allows attackers to bypass intended access restrictions via a crafted	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/195

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

			application, aka internal bug 29189712. **Reference: CVE-2016-3833**		
Bypass	2016-08-05	8.3	The framework APIs 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 2016-08-01 do not ensure that package data originated from the Package Manager, which allows attackers to bypass an unspecified protection mechanism via a crafted application, aka internal bug 28795098. **Reference: CVE-2016-3832**	https://android.googlesource.com/platform/frameworks/base/+/e7cf91a198de995c7440b3b64352effd2e309906	O-GOO-ANDRO--170816/196
Denial of Service	2016-08-05	5	The telephony component 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 2016-08-01 allows remote attackers to cause a denial of service (device crash) via a NITZ time value of 2038-01-19 or later that is mishandled by the system clock, aka internal bug 29083635, related to a "Year 2038 problem." **Reference: CVE-2016-3831**	https://android.googlesource.com/platform/frameworks/opt/telephony/+/f47bc301ccbc5e6d8110afab5a1e9bac1d4ef058	O-GOO-ANDRO--170816/197
Denial of Service	2016-08-05	7.1	codecs/aacdec/SoftAAC2.cpp 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, and 6.x before 2016-08-01 allows	https://android.googlesource.com/platform/frameworks/av/+/8e438e153f661e9df8db0ac41d587e94035	O-GOO-ANDRO--170816/198

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

			remote attackers to cause a denial of service (device hang or reboot) via crafted ADTS data, aka internal bug 29153599. **Reference: CVE-2016-3830**	2df06	
Denial of Service	2016-08-05	7.1	The ih264d decoder in mediaserver in Android 6.x before 2016-08-01 does not initialize certain structure members, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 29023649. **Reference: CVE-2016-3829**	https://android.googlesource.com/platform/external/libavc/+/326fe991a4b7971e8aeaf4ac775491dd8abd85bb	O-GOO-ANDRO--170816/199
Denial of Service	2016-08-05	7.1	decoder/ih264d_api.c in mediaserver in Android 6.x before 2016-08-01 mishandles invalid PPS and SPS NAL units, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28835995. **Reference: CVE-2016-3828**	https://android.googlesource.com/platform/external/libavc/+/7554755536019e439433c515eeb44e701fb3bfb2	O-GOO-ANDRO--170816/200
Denial of Service	2016-08-05	7.1	codecs/hevcdec/SoftHEVC.cpp in libstagefright in mediaserver in Android 6.0.1 before 2016-08-01 mishandles decoder errors, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted	https://android.googlesource.com/platform/frameworks/av/+/a4567c66f4764442c6cb7b5c1858810194480fb5	O-GOO-ANDRO--170816/201

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

			media file, aka internal bug 28816956. **Reference: CVE-2016-3827**		
Gain Privileges	2016-08-05	4.6	services/audioflinger/Effects.cpp 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 2016-08-01 does not validate the reply size for an AudioFlinger effect command, which allows attackers to gain privileges via a crafted application, aka internal bug 29251553. **Reference: CVE-2016-3826**	https://android.googlesource.com/platform/frameworks/av/+/9cd8c3289c91254b3955bd7347cf605d6fa032c6	O-GOO-ANDRO--170816/202
Overflow; Gain Privileges	2016-08-05	4.6	mm-video-v4l2/vidc/venc/src/omx_video_base.cpp in mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allocates an incorrect amount of memory, which allows attackers to gain privileges via a crafted application, aka internal bug 28816964. **Reference: CVE-2016-3825**	https://android.googlesource.com/platform/hardware/qcom/media/+/d575ecf607056d8e3328ef2eb56c52e98f81e87d	O-GOO-ANDRO--170816/203
Overflow; Gain Privileges	2016-08-05	4.6	omx/OMXNodeInstance.cpp 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, and 6.x before 2016-08-01 does not validate the buffer port, which allows attackers to gain privileges via a	https://android.googlesource.com/platform/frameworks/av/+/b351eabb428c7ca85a34513c64601f437923d576	O-GOO-ANDRO--170816/204

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

			crafted application, aka internal bug 28816827. **Reference: CVE-2016-3824**		
Overflow; Gain Privileges	2016-08-05	4.6	The secure-session feature in the mm-video-v4l2 venc component 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 2016-08-01 mishandles heap pointers, which allows attackers to gain privileges via a crafted application, aka internal bug 28815329. **Reference: CVE-2016-3823**	https://android.googlesource.com/platform/hardware/qcom/media/+/7558d03e6498e970b761aa44fff6b2c659202d95	O-GOO-ANDRO--170816/205
Denial of Service; Execute Code; Overflow	2016-08-05	7.5	exif.c in Matthias Wandel jhead 2.87, as used in libjhead 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 2016-08-01, allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds access) via crafted EXIF data, aka internal bug 28868315. **Reference: CVE-2016-3822**	https://android.googlesource.com/platform/external/jhead/+/bae671597d47b9e5955c4cb742e468cebfd7ca6b	O-GOO-ANDRO--170816/206
Denial of Service; Execute Code; Memory Corruption	2016-08-05	7.5	libmedia 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 2016-08-01 has certain incorrect declarations, which allows remote attackers to execute arbitrary code or cause a denial of service (NULL pointer	https://android.googlesource.com/platform/frameworks/av/+/42a25c46b844518ff0d0b920c20c519e1417be69	O-GOO-ANDRO--170816/207

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

			dereference or memory corruption) via a crafted media file, aka internal bug 28166152. **Reference: CVE-2016-3821**		
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-05	7.5	The ih264d decoder in mediaserver in Android 6.x before 2016-08-01 mishandles slice numbers, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28673410. **Reference: CVE-2016-3820**	https://android.googlesource.com/platform/external/libavc/+/a78887bcffbc2995cf9ed72e0697acf560875e9e	O-GOO-ANDRO--170816/208
Denial of Service; Execute Code; Overflow; Memory Corruption	2016-08-05	7.5	Integer overflow in codecs/on2/h264dec/source/h264bsd_dpb.c 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, and 6.x before 2016-08-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28533562. **Reference: CVE-2016-3819**	https://android.googlesource.com/platform/frameworks/av/+/590d1729883f700ab905cdc9ad850f3ddd7e1f56	O-GOO-ANDRO--170816/209
Gain Privileges	2016-08-05	6.9	The Qualcomm GPU driver in Android before 2016-08-05 on Nexus 5, 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/210

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

			Android internal bug 28026365 and Qualcomm internal bug CR1002974. **Reference: CVE-2016-2504**		
Overflow	2016-08-05	7.5	services/core/java/com/android/server/pm/PackageManagerService.java in the framework APIs 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 2016-08-01 allows attackers to increase intent-filter priority via a crafted application, aka internal bug 27450489. **Reference: CVE-2016-2497**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/211
Execute Code; Overflow	2016-08-05	10	Buffer overflow in CORE/SYS/legacy/src/utils/src/dot11f.c in the Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices allows remote attackers to execute arbitrary code via a crafted Information Element (IE) in an 802.11 management frame, aka Android internal bug 28668638 and Qualcomm internal bugs CR553937 and CR553941. **Reference: CVE-2014-9902**	https://source.codeaurora.org/quic/la/platform/vendor/qcom-opensource/wlan/prima/commit/?id=3b1c44a3a7129dc25abe2c23543f6f66c59e8f50	O-GOO-ANDRO--170816/212
Denial of Service	2016-08-05	7.8	The Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices makes incorrect snprintf calls,	https://source.codeaurora.org/quic/la/platform/vendor/qcom-	O-GOO-ANDRO--170816/213

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

			which allows remote attackers to cause a denial of service (device hang or reboot) via crafted frames, aka Android internal bug 28670333 and Qualcomm internal bug CR548711. **Reference: CVE-2014-9901**	opensource/wlan/prima/commit/?id=637f0f7931dd7265ac1c250dc2884d6389c66bde	
Denial of Service	2016-08-06	6.8	netd in Android before 2016-08-05 mishandles tethering and stdio streams, which allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted application, aka Qualcomm internal bug CR959631. **Reference: CVE-2016-3856**	https://source.codeaurora.org/quic/la/platform/system/netd/commit/?h=LA.BR.1&id=568ef402f6d5a7a50c126aafc78c4edf59abba1c	O-GOO-ANDRO--170816/214
Denial of Service	2016-08-06	6.8	drivers/thermal/supply_lm_core.c in the Qualcomm components in Android before 2016-08-05 does not validate a certain count parameter, which allows attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted application, aka Qualcomm internal bug CR990824. **Reference: CVE-2016-3855**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/215
Denial of Service	2016-08-06	6.8	drivers/media/video/msm/msm_mctl_buf.c in the Qualcomm components in Android	http://source.android.com/security/bulletin/2016-08-	O-GOO-ANDRO--170816/216

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

			before 2016-08-05 does not validate the image mode, which allows attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via a crafted application, aka Qualcomm internal bug CR897326. **Reference: CVE-2016-3854**	01.html	
Gain Privileges	2016-08-06	6.8	drivers/video/msm/mdss/mdss_mdp_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not verify that a mapping exists before proceeding with an unmap operation, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28815158 and Qualcomm internal bugs CR794217 and CR836226. **Reference: CVE-2015-8943**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/217
Gain Privileges	2016-08-06	9.3	drivers/media/platform/msm/camera_v2/pproc/cpp/msm_cpp.c in the Qualcomm components in Android before 2016-08-05 on Nexus 6 devices does not validate the stream state, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28814652 and Qualcomm internal	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/218

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

			bug CR803246. **Reference: CVE-2015-8942**		
Gain Privileges	2016-08-06	9.3	drivers/media/platform/msm/camera_v2/isp/msm_isp_axi_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices does not properly validate array indexes, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28814502 and Qualcomm internal bug CR792473. **Reference: CVE-2015-8941**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/219
Overflow; Gain Privileges	2016-08-06	9.3	Integer overflow in sound/soc/msm/qdsp6v2/q6lsm.c in the Qualcomm components in Android before 2016-08-05 on Nexus 6 devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28813987 and Qualcomm internal bug CR792367. **Reference: CVE-2015-8940**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/220
Gain Privileges	2016-08-06	9.3	drivers/video/msm/mdp4_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not validate r stages, g stages, or b stages data, which allows attackers to gain privileges via a crafted	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/221

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

			application, aka Android internal bug 28398884 and Qualcomm internal bug CR779021. **Reference: CVE-2015-8939**		
Gain Privileges	2016-08-06	9.3	The MSM camera driver in the Qualcomm components in Android before 2016-08-05 on Nexus 6 devices does not validate input parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28804030 and Qualcomm internal bug CR766022. **Reference: CVE-2015-8938**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/222
Gain Privileges	2016-08-06	6.8	drivers/char/diag/diagchar_core.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5, 6, and 7 (2013) devices mishandles a socket process, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28803962 and Qualcomm internal bug CR770548. **Reference: CVE-2015-8937**	https://source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=c66202b9288cc4ab1c38f7c928fa1005c285c170	O-GOO-ANDRO--170816/223
Gain Information	2016-08-06	4.3	drivers/usb/host/ehci-msm2.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices omits certain minimum calculations before copying data,	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/224

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

			which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28803909 and Qualcomm internal bug CR547910. **Reference: CVE-2014-9899**		
Gain Information	2016-08-06	4.3	arch/arm/mach-msm/qdsp6v2/ultrasound/usf.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not properly validate input parameters, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28814690 and Qualcomm internal bug CR554575. **Reference: CVE-2014-9898**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/225
Gain Information	2016-08-06	4.3	sound/soc/msm/qdsp6v2/msm-lsm-client.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not validate certain user-space data, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28769856 and Qualcomm internal bug CR563752. **Reference: CVE-2014-9897**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/226
Gain	2016-08-06	4.3	drivers/char/adsprpc.c	http://source.a	O-GOO-

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

Information			in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not properly validate parameters and return values, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28767593 and Qualcomm internal bug CR551795. **Reference: CVE-2014-9896**	ndroid.com/security/bulletin/2016-08-01.html	ANDRO--170816/227
Gain Information	2016-08-06	4.3	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not ensure that certain name strings end in a '\0' character, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28749708 and Qualcomm internal bug CR545736. **Reference: CVE-2014-9894**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/228
Gain Information	2016-08-06	4.3	drivers/video/msm/mdss/mdss_mdp_pp.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not properly determine the size of Gamut LUT data, which allows attackers to obtain sensitive information via a crafted	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/229

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

			application, aka Android internal bug 28747914 and Qualcomm internal bug CR542223. **Reference: CVE-2014-9893**		
Gain Privileges	2016-08-06	9.3	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not validate certain buffer addresses, which allows attackers to gain privileges via a crafted application that makes an ioctl call, aka Android internal bug 28749283 and Qualcomm internal bug CR550061. **Reference: CVE-2014-9891**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/230
Gain Privileges	2016-08-06	9.3	Off-by-one error in drivers/media/platform/msm/camera_v2/sensor/cci/msm_cci.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application that sends an I2C command, aka Android internal bug 28770207 and Qualcomm internal bug CR529177. **Reference: CVE-2014-9890**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/231
Gain Privileges	2016-08-06	6.8	drivers/media/platform/msm/camera_v2/pproc/cpp/msm_cpp.c in the Qualcomm components in Android before 2016-	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/232

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

			08-05 on Nexus 5 devices does not validate CPP frame messages, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28803645 and Qualcomm internal bug CR674712. **Reference: CVE-2014-9889**		
Gain Privileges	2016-08-06	9.3	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain length values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28804057 and Qualcomm internal bug CR636633. **Reference: CVE-2014-9887**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/233
Gain Privileges	2016-08-06	6.8	arch/arm/mach-msm/qdsp6v2/ultrasound/usf.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not properly validate input parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28815575 and Qualcomm internal bug CR555030. **Reference: CVE-2014-9886**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/234

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

Gain Privileges	2016-08-06	6.8	Format string vulnerability in drivers/thermal/qpnp-adc-tm.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices allows attackers to gain privileges via a crafted application that provides format string specifiers in a name, aka Android internal bug 28769959 and Qualcomm internal bug CR562261. **Reference: CVE-2014-9885**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/235
Gain Privileges	2016-08-06	6.8	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain pointers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769920 and Qualcomm internal bug CR580740. **Reference: CVE-2014-9884**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/236
Overflow; Gain Privileges; Gain Information	2016-08-06	6.8	Integer overflow in drivers/char/diag/diag_dci.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges or obtain sensitive information via a crafted application, aka Android internal bug 28769912	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/237

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

			and Qualcomm internal bug CR565160. **Reference: CVE-2014-9883**		
Overflow; Gain Privileges	2016-08-06	6.8	Buffer overflow in drivers/media/radio/radio-iris.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28769546 and Qualcomm internal bug CR552329. **Reference: CVE-2014-9882**	https://source.codeaurora.org/quic/la/kernel/msm/commit/?id=3a4ebaac557a9e3fbcbab4561650abac8298a4d9	O-GOO-ANDRO--170816/238
Denial of Service; Overflow; Gain Privileges	2016-08-06	6.8	drivers/media/radio/radio-iris.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices uses an incorrect integer data type, which allows attackers to gain privileges or cause a denial of service (buffer overflow) via a crafted application, aka Android internal bug 28769368 and Qualcomm internal bug CR539008. **Reference: CVE-2014-9881**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/239
Gain Privileges	2016-08-06	6.8	drivers/video/msm/vidc/common/enc/venc.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not validate VEN_IOCTL_GET_SEQUENCE_HDR ioctl calls,	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/240

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

			which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769352 and Qualcomm internal bug CR556356. **Reference: CVE-2014-9880**		
Gain Privileges	2016-08-06	6.8	The mdss mdp3 driver in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not validate user-space data, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769221 and Qualcomm internal bug CR524490. **Reference: CVE-2014-9879**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/241
Gain Privileges	2016-08-06	6.8	drivers/mmc/card/mmc_block_test.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not reject kernel-space buffer addresses, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769208 and Qualcomm internal bug CR547479. **Reference: CVE-2014-9878**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/242
Gain Privileges	2016-08-06	6.8	drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/243

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

			before 2016-08-05 on Nexus 5 and 7 (2013) devices mishandles a user-space pointer, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28768281 and Qualcomm internal bug CR547231. **Reference: CVE-2014-9877**		
Gain Privileges	2016-08-06	6.8	drivers/char/diag/diagfwd.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5, 5X, 6, 6P, and 7 (2013) devices mishandles certain integer values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28767796 and Qualcomm internal bug CR483408. **Reference: CVE-2014-9876**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/244
Gain Privileges	2016-08-06	6.8	drivers/char/diag/diag_dci.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application that sends short DCI request packets, aka Android internal bug 28767589 and Qualcomm internal bug CR483310. **Reference: CVE-2014-9875**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/245
Overflow; Gain	2016-08-06	6.8	Buffer overflow in the	http://source.a	O-GOO-

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

Privileges			Qualcomm components in Android before 2016-08-05 on Nexus 5, 5X, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, related to arch/arm/mach-msm/qdsp6v2/audio_utils.c and sound/soc/msm/qdsp6v2/q6asm.c, aka Android internal bug 28751152 and Qualcomm internal bug CR563086. **Reference: CVE-2014-9874**	ndroid.com/security/bulletin/2016-08-01.html	ANDRO--170816/246
Gain Privileges; Gain Information	2016-08-06	6.8	Integer underflow in drivers/char/diag/diag_dci.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges or obtain sensitive information via a crafted application, aka Android internal bug 28750726 and Qualcomm internal bug CR556860. **Reference: CVE-2014-9873**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/247
Gain Privileges	2016-08-06	6.8	The diag driver in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not ensure unique identifiers in a DCI client table, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28750155 and Qualcomm internal	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/248

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

			bug CR590721. **Reference: CVE-2014-9872**		
Overflow; Gain Privileges	2016-08-06	9.3	Multiple buffer overflows in drivers/media/platform/msm/camera_v2/isp/msm_isp_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28749803 and Qualcomm internal bug CR514717. **Reference: CVE-2014-9871**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/249
Gain Privileges	2016-08-06	9.3	drivers/media/platform/msm/camera_v2/isp/msm_isp_stats_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain index values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749728 and Qualcomm internal bug CR514711. **Reference: CVE-2014-9869**	https://source.codeaurora.org/quic/la/kernel/msm/commit/?id=8d1f7531ff379befc129a6447642061e87562bca	O-GOO-ANDRO--170816/250
Gain Privileges	2016-08-06	6.9	drivers/media/platform/msm/camera_v2/sensor/csiphy/msm_csiphy.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013)	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/251

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

			devices allows attackers to gain privileges via an application that provides a crafted mask value, aka Android internal bug 28749721 and Qualcomm internal bug CR511976. **Reference: CVE-2014-9868**		
Gain Privileges	2016-08-06	9.3	drivers/media/platform/msm/camera_v2/isp/msm_isp_axi_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate the number of streams, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749629 and Qualcomm internal bug CR514702. **Reference: CVE-2014-9867**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/252
Gain Privileges	2016-08-06	9.3	drivers/media/platform/msm/camera_v2/sensor/csid/msm_csid.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate a certain parameter, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28747684 and Qualcomm internal bug CR511358. **Reference: CVE-2014-9866**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/253
Gain Privileges	2016-08-06	9.3	drivers/misc/qseecom.c	http://source.a	O-GOO-

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

			in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not properly restrict user-space input, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28748271 and Qualcomm internal bug CR550013. **Reference: CVE-2014-9865**	ndroid.com/security/bulletin/2016-08-01.html	ANDRO--170816/254
Gain Privileges	2016-08-06	9.3	drivers/misc/qseecom.c in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate ioctl calls, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28747998 and Qualcomm internal bug CR561841. **Reference: CVE-2014-9864**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/255
Gain Privileges; Gain Information	2016-08-06	9.3	Integer underflow in the diag driver in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges or obtain sensitive information via a crafted application, aka Android internal bug 28768146 and Qualcomm internal bug CR549470. **Reference: CVE-2014-**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/256

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

			9863		
Bypass	2016-08-07	5	packages/SystemUI/src/com/android/systemui/power/PowerNotificationWarnings.java in Android 5.x allows attackers to bypass a DEVICE_POWER permission requirement via a broadcast intent with the PNW.stopSaver action, aka internal bug 20918350. **Reference: CVE-2015-3854**	https://android.googlesource.com/platform/frameworks/base/+/05e0705177d2078fa9f940ce6df723312cfab976	O-GOO-ANDRO--170816/257
Google;Linux					
Android/Linux Kernel *Android (from its former owner Android, Inc.) is a mobile operating system (OS) currently developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets/The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Gain Privileges	2016-08-06	7.2	The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendmsg system call. **Reference: CVE-2016-3841**	https://github.com/torvalds/linux/commit/45f6fad84cc305103b28d73482b344d7f5b76f39	O-GOO-ANDRO--170816/258
Gain Information	2016-08-06	4.3	The ioresources_init function in kernel/resource.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices, uses weak permissions for /proc/iomem, which allows local users to obtain sensitive information by reading	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/259

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

			this file, aka Android internal bug 28814213 and Qualcomm internal bug CR786116. NOTE: the permissions may be intentional in most non-Android contexts. **Reference: CVE-2015-8944**		
Gain Information	2016-08-06	4.3	The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28803952 and Qualcomm internal bug CR570754. **Reference: CVE-2014-9900**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/260
Gain Information	2016-08-06	4.3	drivers/media/media-device.c in the Linux kernel before 3.11, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly initialize certain data structures, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28750150 and Qualcomm internal bug CR570757, a different vulnerability than CVE-	https://source.codeaurora.org/quic/la/kernel/msm/commit/?id=cc4b26575602e492efd986e9a6ffc4278cee53b5	O-GOO-ANDRO--170816/261

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

			2014-1739. **Reference: CVE-2014-9895**		
Gain Information	2016-08-06	4.3	The snd_compr_tstamp function in sound/core/compress_offload.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly initialize a timestamp data structure, which allows attackers to obtain sensitive information via a crafted application, aka Android internal bug 28770164 and Qualcomm internal bug CR568717. **Reference: CVE-2014-9892**	http://source.android.com/security/bulletin/2016-08-01.html	O-GOO-ANDRO--170816/262
Gain Privileges	2016-08-06	9.3	The Linux kernel before 3.11 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly consider user-space access to the TPIDRURW register, which allows local users to gain privileges via a crafted application, aka Android internal bug 28749743 and Qualcomm internal bug CR561044. **Reference: CVE-2014-9870**	https://source.codeaurora.org/quic/la/kernel/msm/commit/?id=4f57652fcd2dce7741f1ac6dc0417e2f265cd1de	O-GOO-ANDRO--170816/263
Huawei					
Cloudengine 12800 Firmware;Cx600 Firmware;Ne40e Firmware;Ne5000e Firmware;Ptn 6900-2-m8 Firmware					

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

Huawei Technologies Co. Ltd. is a Chinese multinational networking and telecommunications equipment and services company headquartered in Shenzhen, Guangdong. It is the largest telecommunications equipment manufacturer in the world.					
Denial of Service; Execute Code	2016-08-02	7.5	Huawei NE40E and CX600 devices with software before V800R007SPH017; PTN 6900-2-M8 devices with software before V800R007SPH019; NE5000E devices with software before V800R006SPH018; and CloudEngine devices 12800 with software before V100R003SPH010 and V100R005 before V100R005SPH006 allow remote attackers with control plane access to cause a denial of service or execute arbitrary code via a crafted packet. **Reference: CVE-2016-6178**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160713-01-multicast-ldp-fec-stack-en	O-HUA-CLOUD--170816/264
P8 Smartphone Firmware *P8 is a very stylish smartphone from Huawei.*					
Denial of Service; Overflow ; Gain Privileges	2016-08-02	9.3	Buffer overflow in the Wi-Fi driver in Huawei P8 smartphones with software before GRA-CL00C92B363 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6192. **Reference: CVE-2016-6193**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160708-01-smartphone-en	O-HUA-P8 SM--170816/265
Denial of Service; Overflow ; Gain	2016-08-02	9.3	Buffer overflow in the Wi-Fi driver in Huawei P8 smartphones with	http://www.huawei.com/en/psirt/security-	O-HUA-P8 SM--170816/266

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

Privileges			software before GRA-CL00C92B363 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6193. **Reference: CVE-2016-6192**	advisories/huawei-sa-20160708-01-smartphone-en	
IBM					
AIX;Vios *AIX is an open operating system from IBM that is based on a version of UNIX; VIOS (Virtual I/O Server) is a IBM virtualization software product.*					
Gain Information	2016-08-07	4.3	IBM AIX 5.3, 6.1, 7.1, and 7.2 and VIOS 2.2.x do not default to the latest TLS version, which makes it easier for man-in-the-middle attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-0266**	https://aix.software.ibm.com/aix/efixes/security/nettcp_advisory2.asc	O-IBM-AIX;V--170816/267
Juniper					
Junos *Junos OS is the FreeBSD-based operating system used in Juniper Networks hardware routers. It is an operating system that is used in Juniper's routing, switching and security devices.*					
Gain Privileges	2016-08-05	6.9	Juniper Junos OS before 12.1X46-D50 on SRX Series devices reverts to "safe mode" authentication and allows root CLI logins without a password after a failed upgrade to 12.1X46, which might allow local users to gain privileges by leveraging use of the "request system software" command with the "partition" option. **Reference: CVE-2016-**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10753	O-JUN-JUNOS--170816/268

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

			1278		
Denial of Service	2016-08-05	7.1	Juniper Junos OS before 12.1X46-D50, 12.1X47 before 12.1X47-D23, 12.3X48 before 12.3X48-D25, and 15.1X49 before 15.1X49-D40 on a High-End SRX-Series chassis system with one or more Application Layer Gateways (ALGs) enabled allow remote attackers to cause a denial of service (CPU consumption, fab link failure, or flip-flop failovers) via vectors related to in-transit traffic matching ALG rules. **Reference: CVE-2016-1276**	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10751	O-JUN-JUNOS--170816/269
Linux					
Linux Kernel *The Linux kernel is a Unix-like computer operating system kernel.*					
Denial of Service; Overflow ; Gain Privileges	2016-08-06	4.4	Race condition in the ioctl_file_dedupe_range function in fs/ioctl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (heap-based buffer overflow) or possibly gain privileges by changing a certain count value, aka a "double fetch" vulnerability. **Reference: CVE-2016-6516**	https://github.com/torvalds/linux/commit/10eec60ce79187686e052092e5383c99b4420a20	O-LIN-LINUX--170816/270
Denial of Service	2016-08-06	4.7	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to	https://bugzilla.redhat.com/show_bug.cgi?id=1362466	O-LIN-LINUX--170816/271

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

			cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability. **Reference: CVE-2016-6480**		
Denial of Service	2016-08-06	4.9	The filesystem layer in the Linux kernel before 4.5.5 proceeds with post-rename operations after an OverlayFS file is renamed to a self-hardlink, which allows local users to cause a denial of service (system crash) via a rename system call, related to fs/namei.c and fs/open.c. **Reference: CVE-2016-6198**	https://github.com/torvalds/linux/commit/9409e22acdfc9153f88d9b1ed2bd2a5b34d2d3ca	O-LIN-LINUX--170816/272
Denial of Service	2016-08-06	4.9	fs/overlayfs/dir.c in the OverlayFS filesystem implementation in the Linux kernel before 4.6 does not properly verify the upper dentry before proceeding with unlink and rename system-call processing, which allows local users to cause a denial of service (system crash) via a rename system call that specifies a self-hardlink. **Reference: CVE-2016-6197**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=11f3710417d026ea2f4fcf362d866342c5274185	O-LIN-LINUX--170816/273
Overflow; Gain Privileges	2016-08-06	7.2	The apparmor_setprocattr function in security/apparmor/lsm.c in the Linux kernel before 4.6.5 does not	https://github.com/torvalds/linux/commit/30a46a4647fd1df9cf52e43bf467f0d9265096	O-LIN-LINUX--170816/274

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

			validate the buffer size, which allows local users to gain privileges by triggering an AppArmor setprocattr hook. **Reference: CVE-2016-6187**	ca	
Denial of Service	2016-08-06	4.6	net/core/skbuff.c in the Linux kernel 4.7-rc6 allows local users to cause a denial of service (panic) or possibly have unspecified other impact via certain IPv6 socket operations. **Reference: CVE-2016-6162**	https://bugzilla.redhat.com/show_bug.cgi?id=1353538	O-LIN-LINUX--170816/275
Denial of Service	2016-08-06	1.9	Race condition in the ec_device_ioctl_xcmd function in drivers/platform/chrome/cros_ec_dev.c in the Linux kernel before 4.7 allows local users to cause a denial of service (out-of-bounds array access) by changing a certain size value, aka a "double fetch" vulnerability. **Reference: CVE-2016-6156**	https://github.com/torvalds/linux/commit/096cdc6f52225835ff503f987a0d68ef770bb78e	O-LIN-LINUX--170816/276
Bypass	2016-08-06	1.9	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a "double fetch" vulnerability.	https://github.com/torvalds/linux/commit/43761473c254b45883a64441dd0bc85a42f3645c	O-LIN-LINUX--170816/277

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-2016-6136		
Gain Information	2016-08-06	4.3	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for man-in-the-middle attackers to hijack TCP sessions via a blind in-window attack. **Reference: CVE-2016-5696**	https://github.com/torvalds/linux/commit/75ff39ccc1bd5d3c455b6822ab09e533c551f758	O-LIN-LINUX--170816/278
Denial of Service; Overflow	2016-08-06	4.9	Memory leak in the airspy_probe function in drivers/media/usb/airspy/airspy.c in the airspy USB driver in the Linux kernel before 4.7 allows local users to cause a denial of service (memory consumption) via a crafted USB device that emulates many VFL_TYPE_SDR or VFL_TYPE_SUBDEV devices and performs many connect and disconnect operations. **Reference: CVE-2016-5400**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=aa93d1fee85c890a34f2510a310e55ee76a27848	O-LIN-LINUX--170816/279
Gain Privileges	2016-08-06	7.2	arch/arm/mm/dma-mapping.c in the Linux kernel before 3.13 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not prevent executable DMA mappings, which might allow local users to gain privileges via a crafted application, aka Android internal bug 28803642	https://source.codeaurora.org/quic/la/kernel/msm/commit/?id=f044936caab337a4384fbfe64a4cbae33c7e22a1	O-LIN-LINUX--170816/280

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

			and Qualcomm internal bug CR642735. **Reference: CVE-2014-9888**		
Bypass	2016-08-07	7.2	The is_ashmem_file function in drivers/staging/android/ashmem.c in a certain Qualcomm Innovation Center (QuIC) Android patch for the Linux kernel 3.x mishandles pointer validation within the KGSL Linux Graphics Module, which allows attackers to bypass intended access restrictions by using the /ashmem string as the dentry name. **Reference: CVE-2016-5340**	https://source.codeaurora.org/quic/la/kernel/msm-3.10/commit/?id=06e51489061e5473b4e2035c79dcf7c27a6f75a6	O-LIN-LINUX--170816/281
Denial of Service; Memory corruption	2016-08-07	10	sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (out-of-bounds write and memory corruption) or possibly have unspecified other impact via a crafted application that makes an ioctl call triggering incorrect use of a parameters pointer. **Reference: CVE-2016-2065**	https://us.codeaurora.org/cgit/quic/la/kernel/msm-3.18/commit/?id=775fca8289eff931f91ff6e8c36cf2034ba59e88	O-LIN-LINUX--170816/282

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	2016-08-07	7.2	sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted application that makes an ioctl call specifying many commands. **Reference: CVE-2016-2064**	https://us.codeaurora.org/cgit/quic/la/kernel/msm-3.18/commit/?id=775fca8289eff931f91ff6e8c36cf2034ba59e88	O-LIN-LINUX--170816/283
Denial of Service; Overflow	2016-08-07	10	Stack-based buffer overflow in the supply_lm_input_write function in drivers/thermal/supply_lm_core.c in the MSM Thermal driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted application that sends a large amount of data through the debugfs interface. **Reference: CVE-2016-2063**	https://www.codeaurora.org/stack-overflow-msm-thermal-driver-allows-kernel-memory-corruption-cve-2016-2063	O-LIN-LINUX--170816/284
Denial of Service	2016-08-07	10	drivers/media/platform	https://us.code	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**

			/msm/broadcast/tsc.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via a crafted application that makes a TSC_GET_CARD_STATUS ioctl call. **Reference: CVE-2015-0573**	aurora.org/cgit/quic/la//kernel/msm-3.10/commit/?id=e20f20aaed6b6d2fd1667bad9be9ef35103a51df	-170816/285
Denial of Service; Gain privileges; Memory corruption	2016-08-07	7.2	Use-after-free vulnerability in the msm_set_crop function in drivers/media/video/msm/msm_camera.c in the MSM-Camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call. **Reference: CVE-2015-0568**	https://www.codeaurora.org/projects/security-advisories/multiple-issues-camera-drivers-cve-2014-9410-cve-2015-0568	O-LIN-LINUX--170816/286
Denial of Service; Gain privileges; Memory	2016-08-07	7.2	The vfe31_proc_general function in drivers/media/video/msm/vfe/msm_vfe31.c in	https://www.codeaurora.org/projects/security-	O-LIN-LINUX--170816/287

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

corruption			the MSM-VFE31 driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate a certain id value, which allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call. **Reference: CVE-2014-9410**	advisories/multiple-issues-camera-drivers-cve-2014-9410-cve-2015-0568	
Microsoft					
Windows 10 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft.*					
Gain Information	2016-08-09	5	ActiveSyncProvider in Microsoft Windows 10 Gold and 1511 allows attackers to discover credentials by leveraging failure of Universal Outlook to obtain a secure connection, aka "Universal Outlook Information Disclosure Vulnerability." **Reference: CVE-2016-3312**	https://technet.microsoft.com/library/security/ms16-103	O-MIC-WINDO--170816/288
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Vista *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft.*					
Gain Privileges	2016-08-09	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2; Windows	http://technet.microsoft.com/en-	O-MIC-WINDO--170816/289

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

			Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3309, and CVE-2016-3310. **Reference: CVE-2016-3311**	us/security/bulletin/ms16-098	
Gain Privileges	2016-08-09	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3309, and CVE-2016-3311. **Reference: CVE-2016-3310**	http://technet.microsoft.com/en-us/security/bulletin/ms16-098	O-MIC-WINDO--170816/290
Gain Privileges	2016-08-09	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows	http://technet.microsoft.com/en-us/security/bulletin/ms16-098	O-MIC-WINDO--170816/291

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

			Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3310, and CVE-2016-3311. **Reference: CVE-2016-3309**		
Gain Privileges	2016-08-09	7.2	The kernel-mode drivers in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3309, CVE-2016-3310, and CVE-2016-3311. **Reference: CVE-2016-3308**	http://technet.microsoft.com/en-us/security/bulletin/ms16-098	O-MIC-WINDO--170816/292
Windows 10;Windows 7;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Vista *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft; Windows Vista (codenamed Longhorn[7]) is an operating system by Microsoft for use on personal computers, including home and business desktops, laptops, tablet PCs and media center PCs.*					
Bypass	2016-08-09	4.3	Microsoft Windows Vista SP2, Windows	https://technet.microsoft.com	O-MIC-WINDO--

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

			Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow remote attackers to hijack network traffic or bypass intended Enhanced Protected Mode (EPM) or application container protection mechanisms, and consequently render untrusted content in a browser, by leveraging how NetBIOS validates responses, aka "NetBIOS Spoofing Vulnerability." **Reference: CVE-2016-3299**	/library/security/ms16-077	170816/293
Bypass	2016-08-09	6.9	Kerberos in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607 allows man-in-the-middle attackers to bypass authentication via vectors related to a fallback to NTLM authentication during a domain account password change, aka "Kerberos Security Feature Bypass Vulnerability." **Reference: CVE-2016-3237**	https://technet.microsoft.com/library/security/ms16-101	O-MIC-WINDO--170816/294

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

Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2012 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft.*					
Bypass	2016-08-09	4	Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold and 1511 allow attackers to bypass the Secure Boot protection mechanism by leveraging (1) administrative or (2) physical access to install a crafted boot manager, aka "Secure Boot Security Feature Bypass." **Reference: CVE-2016-3320**	https://technet.microsoft.com/library/security/ms16-100	O-MIC-WINDO--170816/295
Windows 8.1;Windows Rt 8.1;Windows Server 2012 *Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft; Windows RT is a discontinued operating system for mobile devices developed by Microsoft; Windows Server is a brand name for a group of server operating systems released by Microsoft.*					
Gain Privileges	2016-08-09	7.2	The Netlogon service in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 improperly establishes secure communications channels, which allows local users to gain privileges by leveraging access to a domain-joined machine, aka "Netlogon Elevation of Privilege Vulnerability." **Reference: CVE-2016-3300**	https://technet.microsoft.com/library/security/ms16-101	O-MIC-WINDO--170816/296
Paloaltonetworks					
Pan-os					

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

Panos is a discontinued computer operating system developed by Acorn Computers in the 1980s, which ran on the 32016 Second Processor for the BBC Micro and the Acorn Cambridge Workstation.					
Gain Privileges	2016-08-02	7.2	Palo Alto Networks PAN-OS before 5.0.19, 5.1.x before 5.1.12, 6.0.x before 6.0.14, 6.1.x before 6.1.12, and 7.0.x before 7.0.8 might allow local users to gain privileges by leveraging improper sanitization of the root_reboot local invocation. **Reference: CVE-2016-1712**	http://securityadvisories.paloaltonetworks.com/Home/Detail/45	O-PAL-PAN-O--170816/297
Redhat					
Enterprise Linux Server;Enterprise Linux Workstation *Debian is an operating system and a distribution of Free Software; libcurl is a free and easy-to-use client-side URL transfer library, supporting DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, POP3, POP3S, RTMP, RTSP, SCP, SFTP, SMTP, SMTPS, Telnet and TFTP.*					
Execute Code; Overflow	2016-08-10	7.5	Stack-based buffer overflow in the munge_other_line function in cachemgr.cgi in the squid package before 3.1.23-16.el6_8.6 in Red Hat Enterprise Linux 6 allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-4051. **Reference: CVE-2016-5408**	http://rhn.redhat.com/errata/RHSA-2016-1573.html	O-RED-ENTER--170816/298

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