Vulnerability Type(s)	Publish Date	CVSS	Description	Patch	NCIIPC ID
Application (A)					
Adobe					
Acrobat; Acrobat Dc; Acrobat Reader Dc; Reader *Adobe Acrobat Reader DC software is the free global standard for reliably viewing, printing, and commenting on PDF documents.*					
Execute Code	2016-09-19	10	Use-after-free vulnerability in Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4255. **Reference: CVE-2016-6938**	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-101016/01
Denial of Service; Execute Code Overflow; Memory Corruption	2016-09-30	10	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a	https://helpx.adobe.com/security/products/acrobat/apsb16-26.html	A-ADO-ACROB-101016/02

			different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270. **Reference: CVE-2016-6937**		
Air Sdk & Compiler *Adobe AIR SDK & Compiler provides developers with a consistent and flexible development environment for the delivery of out-of-browser applications and games across devices and platforms (Windows, Mac, iOS, Android).*					
Gain Information	2016-09-22	5	Adobe AIR SDK & Compiler before 23.0.0.257 on Windows does not support Android runtime-analytics transport security, which might allow remote attackers to obtain sensitive information by leveraging access to a network over which analytics data is sent.	https://helpx.adobe.com/security/products/air/apsb16-31.html	A-ADO-AIR S-101016/03

			Reference: CVE-2016-6936		
Digital Editions Adobe Digital Editions is an e-book reader software program from Adobe Systems, built initially using Adobe Flash.					
Execute Code	2016-09-16	10	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-4263**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/04
Denial of Service; Execute Code Overflow; Memory Corruption	2016-09-16	10	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, and CVE-2016-4261. **Reference: CVE-2016-4262**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/05
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-16	10	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, and CVE-2016-4262. **Reference: CVE-2016-4261**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/06
Denial of	2016-09-16	10	Adobe Digital Editions	https://helpx.ad	A-ADO-

Service; Execute Code Overflow; Memory Corruption			before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4261, and CVE-2016-4262. **Reference: CVE-2016-4260**	obe.com/security/products/Digital-Editions/apsb16-28.html	DIGIT-101016/07
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-16	10	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4258, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262. **Reference: CVE-2016-4259**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/08
Denial of Service; Execute Code Overflow; Memory Corruption	2016-09-16	10	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4257, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262. **Reference: CVE-2016-4258**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/09
Denial of	2016-09-16	10	Adobe Digital Editions	https://helpx.ad	A-ADO-

Service; Execute Code Overflow ;Memory Corruption			before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4256, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262. **Reference: CVE-2016-4257**	obe.com/security/products/Digital-Editions/apsb16-28.html	DIGIT-101016/10
Denial of Service; Execute Code Overflow; Memory Corruption	2016-09-16	10	Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4257, CVE-2016-4258, CVE-2016-4259, CVE-2016-4260, CVE-2016-4261, and CVE-2016-4262. **Reference: CVE-2016-4256**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/11
Execute Code	2016-09-30	10	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4263. **Reference: CVE-2016-6980**	https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html	A-ADO-DIGIT-101016/12
Bypass; Gain Information	2016-09-30	5	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on	https://helpx.adobe.com/security/products/flash-player/apsb16-29.html	A-ADO-FLASH-101016/13

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

			Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4277 and CVE-2016-4278, aka a local-with-filesystem Flash sandbox bypass issue. **Reference: CVE-2016-4271**		
Alienvault					
Open Source Security Information And Event Management; Unified Security Management *OSSIM (Open Source Security Information Management) is an open source security information and event management system, integrating a selection of tools designed to aid network administrators in computer security, intrusion detection and prevention; AlienVault Unified Security Management (USM) is an all-in-one platform designed and priced to ensure that mid-market organizations can effectively defend themselves against today's advanced threats.*					
Cross-site scripting	2016-09-28	3.5	Cross-site scripting (XSS) vulnerability in AlienVault OSSIM before 5.3 and USM before 5.3 allows remote attackers to inject arbitrary web script or HTML via the back parameter to ossim/conf/reload.php. **Reference: CVE-2016-6913**	https://www.alienvault.com/forums/discussion/7558/	A-ALI-OPEN - 101016/14
Apache					
Activemq Artemis *Apache ActiveMQ Artemis has a proven non blocking architecture.*					
Execute Code	2016-09-28	6	The getObject method of the javax.jms.ObjectMessage class in the (1) JMS Core client, (2) Artemis broker, and (3) Artemis REST component in Apache ActiveMQ	NA	A-APA-ACTIV-101016/15

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

			Artemis before 1.4.0 might allow remote authenticated users with permission to send messages to the Artemis broker to deserialize arbitrary objects and execute arbitrary code by leveraging gadget classes being present on the Artemis classpath. **Reference: CVE-2016-4978**		
Cxf Fediz *Apache CXF Fediz is a subproject of CXF. Fediz helps you to secure your web applications and delegates security enforcement to the underlying application server.*					
Bypass	2016-09-22	7.5	The application plugins in Apache CXF Fediz 1.2.x before 1.2.3 and 1.3.x before 1.3.1 do not match SAML AudienceRestriction values against configured audience URIs, which might allow remote attackers to have bypass intended restrictions and have unspecified other impact via a crafted SAML token with a trusted signature. **Reference: CVE-2016-4464**	http://cxf.apache.org/security-advisories.data/CVE-2016-4464.txt.asc	A-APA-CXF F-101016/16
Ranger *Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform.*					
Cross-site scripting	2016-09-27	3.5	Cross-site scripting (XSS) vulnerability in the create user functionality in the policy admin tool in Apache Ranger before 0.6.1 allows remote authenticated	https://cwiki.apache.org/confluence/display/RANGER/Vulnerabilities+found+in+Ranger	A-APA-RANGE-101016/17

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

			administrators to inject arbitrary web script or HTML via vectors related to policies. **Reference: CVE-2016-5395**		
Shiro *Shiro is a powerful and easy-to-use Java security framework that performs authentication, authorization, cryptography, and session management.*					
Bypass	2016-09-21	5	Apache Shiro before 1.3.2 allows attackers to bypass intended servlet filters and gain access by leveraging use of a non-root servlet context path. **Reference: CVE-2016-6802**	NA	A-APA-SHIRO-101016/18
Zookeeper *ZooKeeper is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services.*					
Overflow	2016-09-22	6.8	Buffer overflow in the C cli shell in Apache Zookeeper before 3.4.9 and 3.5.x before 3.5.3, when using the "cmd:" batch mode syntax, allows attackers to have unspecified impact via a long command string. **Reference: CVE-2016-5017**	https://git-wip-us.apache.org/repos/asf?p=zookeeper.git;a=commitdiff;h=27ecf981a15554dc8e64a28630af7a5c9e2bdf4f	A-APA-ZOOKE-101016/19
Apple					
ITunes; Safari *A media player by Apple Computer that is used for playing digital music or video files; Safari browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.*					
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iTunes before 12.5.1 on Windows and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service	https://support.apple.com/HT207158	A-APP-ITUNE-101016/20

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

			(memory corruption and application crash) via a crafted web site. **Reference: CVE-2016-4769**		
Safari *Safari is an Apple web browser.*					
NA	2016-09-27	4.3	The Safari Tabs component in Apple Safari before 10 allows remote attackers to spoof the address bar of a tab via a crafted web site. **Reference: CVE-2016-4751**	https://support.apple.com/HT207157	A-APP-SAFAR-101016/21
Xcode *Xcode is an integrated development environment (IDE) containing a suite of software development tools developed by Apple for developing software for macOS.*					
Denial of Service; Overflow; Gain Privileges; Memory Corruption	2016-09-19	7.2	Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4704. **Reference: CVE-2016-4705**	https://support.apple.com/HT207140	A-APP-XCODE-101016/22
Denial of Service; Overflow ; Gain Privileges ;Memory Corruption	2016-09-19	7.2	Apple Xcode before 8 allows local users to gain privileges or cause a denial of service (memory corruption and application crash) via unspecified vectors, a different vulnerability than CVE-2016-4705. **Reference: CVE-2016-4704**	https://support.apple.com/HT207140	A-APP-XCODE-101016/23
Apple; Google					
Safari/Chrome/Edge; Internet Explorer/Firefox/Opera *Safari / Chrome / Edge / Internet Explorer / Firefox / Opera are browsers (a browser is an application*					

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

program that provides a way to look at and interact with all the information on the World Wide Web).					
Gain Information	2016-09-26	5	The HTTP/2 protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack. **Reference: CVE-2016-7153**	NA	A-APP-SAFAR-101016/24
Gain Information	2016-09-26	5	The HTTPS protocol does not consider the role of the TCP congestion window in providing information about content length, which makes it easier for remote attackers to obtain cleartext data by leveraging a web-browser configuration in which third-party cookies are sent, aka a "HEIST" attack. **Reference: CVE-2016-7152**	NA	A-APP-SAFAR-101016/25
NA	2016-09-21	6.8	The TLS protocol 1.2 and earlier supports the rsa_fixed_dh, dss_fixed_dh, rsa_fixed_ecdh, and ecdsa_fixed_ecdh values for ClientCertificateType but does not directly document the ability to compute the master secret in certain	NA	A-APP-SAFAR-101016/26

			situations with a client secret key and server public key but not a server secret key, which makes it easier for man-in-the-middle attackers to spoof TLS servers by leveraging knowledge of the secret key for an arbitrary installed client X.509 certificate, aka the "Key Compromise Impersonation (KCI)" issue. **Reference: CVE-2015-8960**		
Aternity					
Aternity *Aternity provides powerful Application Performance Management and End User Monitoring tools to reduce business disruptions and increase user productivity.*					
Execute Code	2016-09-29	9.3	The web server in Aternity 9 and earlier does not require authentication for getMBeansFromURL loading of Java MBeans, which allows remote attackers to execute arbitrary Java code by registering MBeans. **Reference: CVE-2016-5062**	http://www.kb.cert.org/vuls/id/706359	A-ATE-ATERN-101016/27
Cross-site scripting	2016-09-29	4.3	Multiple cross-site scripting (XSS) vulnerabilities in the web server in Aternity 9 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) HTTPAgent, (2) MacAgent, (3) getExternalURL, or (4) retrieveTrustedUrl page.	http://www.kb.cert.org/vuls/id/706359	A-ATE-ATERN-101016/28

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-2016-5061		
Cisco					
Application Policy Infrastructure Controller *APIC-EM provides centralized automation of policy-based application profiles. Through programmability, automated network control helps IT rapidly respond to new business opportunities.*					
NA	2016-09-26	6.8	The installation procedure on Cisco Application Policy Infrastructure Controller (APIC) devices 1.3(2f) mishandles binary files, which allows local users to obtain root access via unspecified vectors, aka Bug ID CSCva50496. **Reference: CVE-2016-6413**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-apic	A-CIS-APPLI-101016/29
Carrier Routing System *The Cisco Carrier Routing System provides outstanding economical scale, IP and optical network convergence, and a proven architecture.*					
Denial of Service	2016-09-19	5.7	Cisco Carrier Routing System (CRS) 5.1 and 5.1.4, as used in CRS Carrier Grade Services for CRS-1 and CRS-3 devices, allows remote attackers to cause a denial of service (line-card reload) via crafted IPv6-over-MPLS packets, aka Bug ID CSCva32494. **Reference: CVE-2016-6401**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-crs	A-CIS-CARRI-101016/30
Cloud Services Platform 2100 *Cloud Services Platform 2100 is a turn-key and optimized x86 software and hardware platform for data center Network Functions Virtualization.*					
Execute Code	2016-09-23	7.5	Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote attackers to execute arbitrary code via a crafted	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-CLOUD-101016/31

			dnslookup command in an HTTP request, aka Bug ID CSCuz89093. **Reference: CVE-2016-6374**	20160921-csp2100-2	
Execute Code	2016-09-23	9	The web-based GUI in Cisco Cloud Services Platform (CSP) 2100 2.0 allows remote authenticated administrators to execute arbitrary OS commands as root via crafted platform commands, aka Bug ID CSCva00541. **Reference: CVE-2016-6373**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-csp2100-1	A-CIS-CLOUD-101016/32
Email Security Appliance *Cisco Email Security Appliances defend mission-critical email systems at the gateway, and automatically stop spam, viruses, and other threats.*					
NA	2016-09-23	10	Cisco IronPort AsyncOS 9.1.2-023, 9.1.2-028, 9.1.2-036, 9.7.2-046, 9.7.2-047, 9.7.2-054, 10.0.0-124, and 10.0.0-125 on Email Security Appliance (ESA) devices, when Enrollment Client before 1.0.2-065 is installed, allows remote attackers to obtain root access via a connection to the testing/debugging interface, aka Bug ID CSCvb26017. **Reference: CVE-2016-6406**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160922-esa	A-CIS-EMAIL-101016/33
Firesight System Software *Cisco Firesight System Software centralizes, integrates, and simplifies management. Firesight System Software provides complete and unified management over firewalls, application control, and intrusion prevention, URL filtering, and advanced malware protection.*					

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

Bypass	2016-09-27	5	Cisco Firepower Management Center and FireSIGHT System Software 6.0.1 mishandle comparisons between URLs and X.509 certificates, which allows remote attackers to bypass intended do-not-decrypt settings via a crafted URL, aka Bug ID CSCva50585. **Reference: CVE-2016-6411**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-fmc	A-CIS-FIRES-101016/34
Fog Director *Cisco Fog Director to manage large-scale production deployments of Internet of Things (IoT) application*					
Bypass	2016-09-19	6.8	Cisco Fog Director 1.0(0) for IOx allows remote authenticated users to bypass intended access restrictions and write to arbitrary files via the Cartridge interface, aka Bug ID CSCuz89368. **Reference: CVE-2016-6405**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ioxfd	A-CIS-FOG D-101016/35
Prime Home *Cisco Prime Home provides a feature-rich, standards-based remote management and provisioning solution that provides visibility into the home network reduces operational costs and improves the subscriber experience.*					
NA	2016-09-26	4.3	Cisco Prime Home 5.2.0 allows remote attackers to read arbitrary files via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, aka Bug ID CSCvb17814. **Reference: CVE-2016-6408**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-cph	A-CIS-PRIME-101016/36

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

Unified Computing System *The Cisco Unified Computing System (UCS) is an (x86) architecture data center server product line composed of computing hardware, virtualization support, switching fabric, and management software introduced in 2009.*					
NA	2016-09-19	7.2	UCS Manager and UCS 6200 Fabric Interconnects in Cisco Unified Computing System (UCS) through 3.0(2d) allow local users to obtain OS root access via crafted CLI input, aka Bug ID CSCuz91263. **Reference: CVE-2016-6402**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ucs	A-CIS-UNIFI-101016/37
Web Security Appliance *The Cisco Web Security Appliance (WSA) combines advanced threat defense, advanced malware protection, application visibility and control, insightful reporting, and secure mobility these forms of protection and more in a single solution.*					
Denial of Service	2016-09-19	5	Cisco AsyncOS through 9.5.0-444 on Web Security Appliance (WSA) devices allows remote attackers to cause a denial of service (link saturation) by making many HTTP requests for overlapping byte ranges simultaneously, aka Bug ID CSCuz27219. **Reference: CVE-2016-6407**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-wsa	A-CIS-WEB S-101016/38
Webex Meetings Server *Cisco WebEx server provide a cost-effective, highly secure, high-availability and flexible collaboration and communications solution.*					
Denial of Service	2016-09-19	7.8	Cisco WebEx Meetings Server 2.6 allows remote attackers to cause a denial of service (CPU consumption) by repeatedly accessing the account-validation	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-wms	A-CIS-WEBEX-101016/39

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

			component of an unspecified service, aka Bug ID CSCuy92704. **Reference: CVE-2016-1483**		
Execute Code	2016-09-19	9.3	Cisco WebEx Meetings Server 2.6 allows remote attackers to execute arbitrary commands by injecting these commands into an application script, aka Bug ID CSCuy83130. **Reference: CVE-2016-1482**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-wem	A-CIS-WEBEX-101016/40
Cloud Foundry; Pivotal					
Php Buildpack/Cloud Foundry Elastic Runtime *A Php buildpack to deploy PHP applications to Cloud Foundry based systems, such as a cloud provider;Cloud Foundry is an open platform as a service, providing a choice of clouds, developer frameworks, and application services.*					
Gain Information	2016-09-19	5	Cloud Foundry PHP Buildpack (aka php-buildpack) before 4.3.18 and PHP Buildpack Cf-release before 242, as used in Pivotal Cloud Foundry (PCF) Elastic Runtime before 1.6.38 and 1.7.x before 1.7.19 and other products, place the .profile file in the htdocs directory, which might allow remote attackers to obtain sensitive information via an HTTP GET request for this file. **Reference: CVE-2016-6639**	https://pivotal.io/security/cve-2016-6639	A-CLO-PHP B-101016/41
Cryptopp					
Crypto++ *Crypto++ Library is a free C++ class library of cryptographic schemes.*					
Gain	2016-09-16	4.3	Crypto++ (aka	https://github.c	A-CRY-

Information			cryptopp) through 5.6.4 does not document the requirement for a compile-time NDEBUG definition disabling the many assert calls that are unintended in production use, which might allow context-dependent attackers to obtain sensitive information by leveraging access to process memory after an assertion failure, as demonstrated by reading a core dump. **Reference: CVE-2016-7420**	om/weidai11/cryptopp/issues/277	CRYPT-101016/42
Dentsply Sirona					
Cdr Dicom *CDR DICOM is software for managing medical dental records.*					
NA	2016-09-22	10	Dentsply Sirona (formerly Schick) CDR Dicom 5 and earlier has default passwords for the sa and cdr accounts, which allows remote attackers to obtain administrative access by leveraging knowledge of these passwords. **Reference: CVE-2016-6530**	https://www.schickbysirona.com/items.php?itemid=19189	A-DEN-CDRD-101016/43
Dexis					
Imaging Suite *The Imaging Suite provides analytical services to internal, external and industrial clients for experimental applications at micro and nano scale.*					
NA	2016-09-28	10	DEXIS Imaging Suite 10 has a hardcoded password for the sa account, which allows remote attackers to	http://www.kb.cert.org/vuls/id/282991	A-DEX-IMAGI-101016/44

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

			obtain administrative access by entering this password in a DEXIS_DATA SQL Server session. **Reference: CVE-2016-6532**		
EMC					
Avamar Server *Avamar Fast, efficient backup and recovery through a complete software and hardware solution.*					
NA	2016-09-21	7.2	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain root privileges by leveraging admin access and entering a sudo command. **Reference: CVE-2016-0905**	http://seclists.org/bugtraq/2016/Sep/31	A-EMC-AVAMA-101016/45
Gain Information	2016-09-21	5	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 use the same encryption key across different customers' installations, which allows remote attackers to defeat cryptographic protection mechanisms and obtain sensitive client-server traffic information by leveraging knowledge of this key from another installation. **Reference: CVE-2016-0904**	http://seclists.org/bugtraq/2016/Sep/31	A-EMC-AVAMA-101016/46

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	2016-09-21	6.4	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 rely on client-side authentication, which allows remote attackers to spoof clients and read backup data via a modified client agent. **Reference: CVE-2016-0903**	http://seclists.org/bugtraq/2016/Sep/31	A-EMC-AVAMA-101016/47
NA	2016-09-22	6.9	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 use weak permissions for unspecified directories, which allows local users to obtain root access by replacing a script with a Trojan horse program. **Reference: CVE-2016-0921**	http://seclists.org/bugtraq/2016/Sep/31	A-EMC-AVAMA-101016/48
NA	2016-09-22	7.2	Avamar Data Store (ADS) and Avamar Virtual Edition (AVE) in EMC Avamar Server before 7.3.0-233 allow local users to obtain root access via a crafted parameter to a command that is available in the sudo configuration. **Reference: CVE-2016-0920**	http://seclists.org/bugtraq/2016/Sep/31	A-EMC-AVAMA-101016/49
Documentum D2 *EMC Documentum D2 is the advanced, intuitive, and configurable content-centric client for Documentum that accelerates adoption of ECM applications.*					
NA	2016-09-19	5	EMC Documentum D2 4.5 before patch 15 and 4.6 before patch 03	http://seclists.org/bugtraq/2016/Sep/18	A-EMC-DOCUM-101016/50

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

			allows remote attackers to read arbitrary Docbase documents by leveraging knowledge of an r_object_id value. **Reference: CVE-2016-6644**		
RSA Adaptive Authentication On-premise *RSA Adaptive Authentication is a comprehensive authentication and fraud detection platform that leverages RSA's Risk-Based Authentication technology to measure the risk associated with a user's login and post-login activities by evaluating over 100 attributes.*					
Cross-site scripting	2016-09-22	3.5	Cross-site scripting (XSS) vulnerability in the Case Management application in EMC RSA Adaptive Authentication (On-Premise) before 6.0.2.1.SP3.P4 HF210, 7.0.x and 7.1.x before 7.1.0.0.SP0.P6 HF50, and 7.2.x before 7.2.0.0.SP0.P0 HF20 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-0925**	NA	A-EMC-RSA A-101016/51
Rsa Bsafe *RSA BSAFE is a FIPS 140-2 validated cryptography library offered by RSA Security.*					
NA	2016-09-19	2.6	The TLS 1.2 implementation in EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x before 4.0.9 and 4.1.x before 4.1.5 supports MD5 signatures, which makes it easier for man-in-the-middle attackers to impersonate clients via a transcript-collision attack.	NA	A-EMC-RSA B-101016/52

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-2016-0924		
NA	2016-09-20	2.6	The client in EMC RSA BSAFE Micro Edition Suite (MES) 4.0.x before 4.0.9 and 4.1.x before 4.1.5 places the weakest algorithms first in a signature-algorithm list transmitted to a server, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging server behavior in which the first algorithm is used. **Reference: CVE-2016-0923**	http://seclists.org/bugtraq/2016/Sep/25	A-EMC-RSA B-101016/53
Rsa Identity Management And Governance; Rsa Via Lifecycle And Governance *Rsa Identity Management And Governance is designed to protect enterprises against attacks involving rogue access points through integrated identity management that covers all systems and users; RSA Via Lifecycle and Governance platform helps organizations efficiently meet their security, regulatory and business access needs through a collaborative set of business processes.*					
Gain Information	2016-09-26	4	EMC RSA Identity Management and Governance before 6.8.1 P25 and 6.9.x before 6.9.1 P15 and RSA Via Lifecycle and Governance before 7.0.0 P04 allow remote authenticated users to obtain User Detail Popup information via a modified URL. **Reference: CVE-2016-0918**	http://seclists.org/bugtraq/2016/Sep/52	A-EMC-RSA I-101016/54
Vipr Srm *ViPR SRM is storage resource management software that enables IT to visualize storage relationships, analyze configurations and capacity growth, and optimize resources to improve return on investment (ROI) in traditional and software-defined storage environments.*					
Cross-site scripting	2016-09-19	4.3	Cross-site scripting (XSS) vulnerability in	http://seclists.org/bugtraq/201	A-EMC-VIPR - 101016/55

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

			EMC ViPR SRM before 3.7.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-6643**	6/Sep/17	
Cross Site Request Forgery	2016-09-19	5.8	Cross-site request forgery (CSRF) vulnerability in EMC ViPR SRM before 3.7.2 allows remote attackers to hijack the authentication of administrators for requests that upload files. **Reference: CVE-2016-6642**	http://seclists.org/bugtraq/2016/Sep/17	A-EMC-VIPR - 101016/56
Cross-site scripting	2016-09-19	3.5	Cross-site scripting (XSS) vulnerability in EMC ViPR SRM before 3.7.2 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-6641**	http://seclists.org/bugtraq/2016/Sep/17	A-EMC-VIPR - 101016/57
NA	2016-09-19	5	EMC ViPR SRM before 3.7.2 does not restrict the number of password-authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force guessing attack. **Reference: CVE-2016-0922**	http://seclists.org/bugtraq/2016/Sep/17	A-EMC-VIPR - 101016/58
Cross-site scripting	2016-09-30	3.5	Cross-site scripting (XSS) vulnerability in EMC ViPR SRM before	http://seclists.org/bugtraq/2016/Sep/62	A-EMC-VIPR - 101016/59

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

			4.0.1 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-6647**		
Vnx1 Oe Firmware;Vnx2 Oe Firmware;Vnxe Oe Firmware: *NA*					
Execute Code	2016-09-22	7.5	The SMB service in EMC VNXe, VNX1 File OE before 7.1.80.3, and VNX2 File OE before 8.1.9.155 does not prevent duplicate NTLM challenge-response nonces, which makes it easier for remote attackers to execute arbitrary code, or read or write to files, via a series of authentication requests, a related issue to CVE-2010-0231. **Reference: CVE-2016-0917**	http://seclists.org/bugtraq/2016/Sep/32	A-EMC-VNX1-101016/60
Fortinet					
Fortiwan *FortiWAN intelligently balances Internet and intranet traffic across multiple WAN connections to lower bandwidth costs and keep users connected.*					
Cross-site scripting	2016-09-21	4.3	Cross-site scripting (XSS) vulnerability in Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote attackers to inject arbitrary web script or HTML via the IP parameter to script/statistics/getconn.php. **Reference: CVE-2016-4969**	http://docs.fortinet.com/uploaded/files/3236/fortiwan-v4.2.5-release-notes.pdf	A-FOR-FORTI-101016/61
Gain Information	2016-09-21	4	The linkreport/tmp/admin_	http://docs.fortinet.com/upload	A-FOR-FORTI-

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

			global page in Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users to discover administrator cookies via a GET request. **Reference: CVE-2016-4968**	ed/files/3236/fortiwan-v4.2.5-release-notes.pdf	101016/62
Gain Information	2016-09-21	4	Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users to obtain sensitive information from (1) a backup of the device configuration via script/cfg_show.php or (2) PCAP files via script/system/tcpdump.php. **Reference: CVE-2016-4967**	http://docs.fortinet.com/uploaded/files/3236/fortiwan-v4.2.5-release-notes.pdf	A-FOR-FORTI-101016/63
NA	2016-09-21	4	The diagnosis_control.php page in Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users to download PCAP files via vectors related to the UserName GET parameter. **Reference: CVE-2016-4966**	http://docs.fortinet.com/uploaded/files/3236/fortiwan-v4.2.5-release-notes.pdf	A-FOR-FORTI-101016/64
Execute Code	2016-09-21	9	Fortinet FortiWan (formerly AscernLink) before 4.2.5 allows remote authenticated users with access to the nslookup functionality to execute arbitrary commands with root	http://docs.fortinet.com/uploaded/files/3236/fortiwan-v4.2.5-release-notes.pdf	A-FOR-FORTI-101016/65

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

			privileges via the graph parameter to diagnosis_control.php. **Reference: CVE-2016-4965**		
GNU					
Gnutls *GnuTLS is a secure communications library implementing the SSL, TLS and DTLS protocols and technologies around them*					
Bypass	2016-09-28	5	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc. **Reference: CVE-2016-7444**	https://www.gnutls.org/security.html	A-GNU-GNUTL-101016/66
Wget *GNU Wget is a free utility for non-interactive download of files from the Web.*					
Bypass	2016-09-28	6.8	Race condition in wget 1.17 and earlier, when used in recursive or mirroring mode to download a single file, might allow remote servers to bypass intended access list restrictions by keeping an HTTP connection open. **Reference: CVE-2016-7098**	NA	A-GNU-WGET-101016/67
Google					
Chrome *Google Chrome is a Web browser.*					

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

Execute Code Overflow	2016-09-22	6.8	Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to execute arbitrary code via crafted coordinate values in JPEG 2000 data. **Reference: CVE-2016-5157**	https://pdfium.googlesource.com/pdfium/+/b6befb2ed2485a3805cddea86dc7574510178ea9	A-GOO-CHROM-101016/68
Denial of Service	2016-09-27	6.8	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.113 allow attackers to cause a denial of service or possibly have other impact via unknown vectors. **Reference: CVE-2016-5175**	https://googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	A-GOO-CHROM-101016/69
Denial of Service	2016-09-27	4.3	browser/ui/cocoa/browser_window_controller_private.mm in Google Chrome before 53.0.2785.113 does not process fullscreen toggle requests during a fullscreen transition, which allows remote attackers to cause a denial of service (unsuppressed popup) via a crafted web site. **Reference: CVE-2016-5174**	https://googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	A-GOO-CHROM-101016/70
Bypass	2016-09-27	6.8	The extensions	https://googlec	A-GOO-

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

			subsystem in Google Chrome before 53.0.2785.113 does not properly restrict access to Object.prototype, which allows remote attackers to load unintended resources, and consequently trigger unintended JavaScript function calls and bypass the Same Origin Policy via an indirect interception attack. **Reference: CVE-2016-5173**	hromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	CHROM-101016/71
Gain Information	2016-09-27	4.3	The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code. **Reference: CVE-2016-5172**	https://googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	A-GOO-CHROM-101016/72
Denial of Service	2016-09-27	6.8	WebKit/Source/bindings/templates/interface.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not prevent certain constructor calls, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code. **Reference: CVE-2016-**	https://googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	A-GOO-CHROM-101016/73

			5171		
Denial of Service	2016-09-27	6.8	WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not properly consider getter side effects during array key conversion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Indexed Database (aka IndexedDB) API calls. **Reference: CVE-2016-5170**	https://googlechromereleases.blogspot.com/2016/09/stable-channel-update-for-desktop_13.html	A-GOO-CHROM-101016/74
Bypass	2016-09-29	4.3	Google Chrome before 53.0.2785.113 allows remote attackers to bypass the SafeBrowsing protection mechanism via unspecified vectors. **Reference: CVE-2016-5176**	https://crbug.com/595838	A-GOO-CHROM-101016/75
Denial of Service	2016-09-30	6.8	Google Chrome before 53.0.2785.113 does not ensure that the recipient of a certain IPC message is a valid RenderFrame or RenderWidget, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) or possibly have unspecified other impact by leveraging	https://crbug.com/556351	A-GOO-CHROM-101016/76

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

			access to a renderer process, related to render_frame_host_impl .cc and render_widget_host_im pl.cc, as demonstrated by a Password Manager message. **Reference: CVE-2016-7549**		
HP					
Loadrunner; Performance Center *HPE LoadRunner is a software testing tool from Hewlett Packard Enterprise. It is used to test applications, measuring system behaviour and performance under load.;HP Performance Center software is an enterprise-class performance testing platform and framework.*					
Denial of Service	2016-09-21	9	HPE Performance Center before 12.50 and LoadRunner before 12.50 allow remote attackers to cause a denial of service via unspecified vectors. **Reference: CVE-2016-4384**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05278882	A-HP-LOADR-101016/77
Network Automation *Network automation is the use of IT controls to supervise and carry out every-day network management functions.*					
NA	2016-09-29	6.9	HPE Network Automation Software 10.10 allows local users to write to arbitrary files via unspecified vectors. **Reference: CVE-2016-4386**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05281739	A-HP-NETWO-101016/78
Execute Code	2016-09-29	7.5	HP Network Automation Software 9.1x, 9.2x, 10.0x before 10.00.02.01, and 10.1x before 10.11.00.01 allows remote attackers to execute arbitrary commands via a crafted serialized Java object,	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05279098	A-HP-NETWO-101016/79

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

			related to the Apache Commons Collections (ACC) library. **Reference: CVE-2016-4385**		
Performance Center *HPE Performance Center enables enterprise and global application performance testing with standardized processes and resources to create a Testing Center*					
Bypass	2016-09-22	6	HPE Performance Center 11.52, 12.00, 12.01, 12.20, and 12.50 allows remote attackers to bypass intended access restrictions via unspecified vectors, related to a "remote user validation failure" issue. **Reference: CVE-2016-4382**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05269356	A-HP-PERFO-101016/80
Huawei					
Anyoffice Secureapp: *NA*					
Denial of Service	2016-09-28	7.1	Huawei AnyMail before 2.6.0301.0060 allows remote attackers to cause a denial of service (application crash) via a crafted compressed email attachment. **Reference: CVE-2016-6826**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160815-01-anymail-en	A-HUA-ANYOF-101016/81
Fusioncompute *FusionCompute is a fully Huawei in-house developed computing virtualization software.*					
Gain Information	2016-09-28	4	Huawei FusionCompute before V100R005C10CP7002 stores cleartext AES keys in a file, which allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160815-01-fusioncompute-en	A-HUA-FUSIO-101016/82

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

			6827		
Oceanstor Ism *The OceanStor ISM (Integrated Storage Manager) system can manage the storage devices that support the SMI-S standard.*					
Cross-site scripting	2016-09-28	4.3	Cross-site scripting (XSS) vulnerability in the management interface in Huawei OceanStor ISM before V200R001C04SPC200 allows remote attackers to inject arbitrary web script or HTML via the loginName parameter to cgi-bin/doLogin_CgiEntry and possibly other unspecified vectors. **Reference: CVE-2016-6840**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160818-01-ism-en	A-HUA-OCEAN-101016/83
Policy Center *HUAWEI Policy Center employs a policy engine to implement unified access policies for Internet and intranet access via wired or wireless networks.*					
Cross-site scripting	2016-09-28	3.5	Cross-site scripting (XSS) vulnerability in Huawei Policy Center before V100R003C10SPC020 allows remote authenticated users to inject arbitrary web script or HTML via vectors related to "special characters on pages." **Reference: CVE-2016-4058**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160419-01-policycenter-en	A-HUA-POLIC-101016/84
IBM					
Connections *'Connections' allows your organization to engage the right people, accelerate innovation and deliver results.*					
Cross Site Request Forgery	2016-09-26	6.8	Cross-site request forgery (CSRF) vulnerability in IBM	https://www-01.ibm.com/support/docview.w	A-IBM-CONNE-101016/85

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

			Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to hijack the authentication of arbitrary users. **Reference: CVE-2016-3007**	ss?uid=swg21989067	
Cross-site scripting	2016-09-26	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string, a different vulnerability than CVE-2016-3001 and CVE-2016-3003. **Reference: CVE-2016-3006**	https://www-01.ibm.com/support/docview.wss?uid=swg21989067	A-IBM-CONNE-101016/86
Cross-site scripting	2016-09-26	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string, a different vulnerability than CVE-2016-3001 and CVE-2016-3006. **Reference: CVE-2016-3003**	https://www-01.ibm.com/support/docview.wss?uid=swg21989067	A-IBM-CONNE-101016/87
Cross-site scripting	2016-09-26	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM	https://www-01.ibm.com/support/docview.w	A-IBM-CONNE-101016/88

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

			Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string, a different vulnerability than CVE-2016-3003 and CVE-2016-3006. **Reference: CVE-2016-3001**	ss?uid=swg21989067	
Denial of Service	2016-09-26	4	The help service in IBM Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to cause a denial of service (service degradation) via a crafted URL. **Reference: CVE-2016-3000**	https://www-01.ibm.com/support/docview.wss?uid=swg21989067	A-IBM-CONNE-101016/89
Gain Information	2016-09-26	4	IBM Connections 4.x through 4.5 CR5, 5.0 before CR4, and 5.5 before CR1 allows remote authenticated users to obtain sensitive information via an unspecified brute-force attack. **Reference: CVE-2016-2999**	https://www-01.ibm.com/support/docview.wss?uid=swg21989067	A-IBM-CONNE-101016/90
DB2; Db2 Connect *DB2 is a database product from IBM. It is a Relational Database Management System (RDBMS); DB2 Connect provides connectivity to mainframe and midrange databases from Linux, UNIX, and Windows operating systems.*					
Gain Privileges	2016-10-03	6.9	Untrusted search path vulnerability in IBM DB2 9.7 through FP11, 10.1 through FP5, 10.5 before FP8, and 11.1 GA on Linux, AIX, and HP-	http://www-01.ibm.com/support/docview.wss?uid=swg21990061	A-IBM-DB2;D-101016/91

			UX allows local users to gain privileges via a Trojan horse library that is accessed by a setuid or setgid program. **Reference: CVE-2016-5995**		
Security Guardium *Security Guardium Data Activity Monitor prevents unauthorized data access, alerts on changes or leaks to help ensure data integrity, automates compliance controls and protects against internal and external threats.*					
Gain Information	2016-09-26	4.3	IBM Security Guardium 9.0 before p700 and 10.0 before p100 allows man-in-the-middle attackers to obtain sensitive query-string information from SSL sessions via unspecified vectors. **Reference: CVE-2016-0248**	http://www-01.ibm.com/support/docview.wss?uid=swg21982031	A-IBM-SECUR-101016/92
Security Privileged Identity Manager Virtual Appliance *IBM Security Privileged Identity Manager virtual appliance manages privileged sessions, credential access, session recordings, and application identities.*					
Cross-site scripting	2016-09-28	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before 2.0.2 FP8 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string. **Reference: CVE-2016-5974**	http://www-01.ibm.com/support/docview.wss?uid=swg21989205	A-IBM-SECUR-101016/93
Gain Information	2016-09-28	4.9	IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before	http://www-01.ibm.com/support/docview.wss?uid=swg2198	A-IBM-SECUR-101016/94

			2.0.2 FP8 uses weak permissions for unspecified resources, which allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors. **Reference: CVE-2016-5972**	9205	
Denial of Service	2016-09-28	5.5	IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before 2.0.2 FP8 allows remote authenticated users to read arbitrary files or cause a denial of service (memory consumption) via an XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-5971**	http://www-01.ibm.com/support/docview.wss?uid=swg21989205	A-IBM-SECUR-101016/95
Directory Traversal	2016-09-28	4	Directory traversal vulnerability in IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before 2.0.2 FP8 allows remote authenticated users to read arbitrary files via a .. (dot dot) in a URL. **Reference: CVE-2016-5970**	http://www-01.ibm.com/support/docview.wss?uid=swg21989205	A-IBM-SECUR-101016/96
Execute Code	2016-09-28	6.5	IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before	http://www-01.ibm.com/support/docview.wss?uid=swg2198	A-IBM-SECUR-101016/97

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

			2.0.2 FP8 does not properly validate updates, which allows remote authenticated users to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-5963**	9205	
Gain Information	2016-09-28	5	IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before 2.0.2 FP8 allows remote attackers to defeat cryptographic protection mechanisms and obtain sensitive information by leveraging a weak algorithm. **Reference: CVE-2016-5957**	http://www-01.ibm.com/support/docview.wss?uid=swg21989205	A-IBM-SECUR-101016/98
NA	2016-09-28	4.9	IBM WebSphere Application Server (WAS) Liberty, as used in IBM Security Privileged Identity Manager (ISPIM) Virtual Appliance 2.x before 2.0.2 FP8, allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **Reference: CVE-2016-3040**	http://www-01.ibm.com/support/docview.wss?uid=swg21989205	A-IBM-SECUR-101016/99

Spectrum Control; Tivoli Storage Productivity Center

Spectrum Control data management and storage management solutions provide comprehensive monitoring, automation and analytics that can optimize all types of storage; IBM Tivoli Storage Productivity Center is an industry-leading storage resource management software that provides comprehensive visibility, control and automation for managing heterogeneous storage infrastructures through a centralized, web-based management console.

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

NA	2016-09-27	3.5	IBM Spectrum Control (formerly Tivoli Storage Productivity Center) 5.2.x before 5.2.11 allows remote authenticated users to conduct clickjacking attacks via a crafted web site. **Reference: CVE-2016-5947**	http://www-01.ibm.com/support/docview.wss?uid=swg21988625	A-IBM-SPECT-101016/100
Directory Traversal; Gain Information	2016-09-27	4	Directory traversal vulnerability in IBM Spectrum Control (formerly Tivoli Storage Productivity Center) 5.2.x before 5.2.11 allows remote authenticated users to read arbitrary files via a .. (dot dot) in a URL. **Reference: CVE-2016-5946**	http://www-01.ibm.com/support/docview.wss?uid=swg21988625	A-IBM-SPECT-101016/101
NA	2016-09-27	4	IBM Spectrum Control (formerly Tivoli Storage Productivity Center) 5.2.x before 5.2.11 allows remote authenticated users to upload non-executable files via a crafted HTTP request. **Reference: CVE-2016-5945**	http://www-01.ibm.com/support/docview.wss?uid=swg21988625	A-IBM-SPECT-101016/102
Cross-site scripting	2016-09-27	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM Spectrum Control (formerly Tivoli Storage Productivity Center) 5.2.x before 5.2.11 allows remote authenticated users to inject arbitrary web script or HTML via an	http://www-01.ibm.com/support/docview.wss?uid=swg21988625	A-IBM-SPECT-101016/103

			embedded string. **Reference: CVE-2016-5944**		
Bypass	2016-09-27	5.5	IBM Spectrum Control (formerly Tivoli Storage Productivity Center) 5.2.x before 5.2.11 allows remote authenticated users to bypass intended access restrictions, and read task details or edit properties, via unspecified vectors. **Reference: CVE-2016-5943**	http://www-01.ibm.com/support/docview.wss?uid=swg21988625	A-IBM-SPECT-101016/104
Tealeaf Customer Experience *IBM Tealeaf customer experience management solutions provide critical visibility, insight and answers to help companies meet online conversion and customer retention*					
NA	2016-09-27	4	The web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049 FP9, 9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before 9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 does not apply password-quality rules to password changes, which makes it easier for remote attackers to obtain access via a brute-force attack. **Reference: CVE-2016-5997**	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/105
NA	2016-09-27	5	The web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049 FP9,	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/106

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

			9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before 9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 does not enforce password-length restrictions, which makes it easier for remote attackers to obtain access via a brute-force attack. **Reference: CVE-2016-5996**		
Cross-site scripting	2016-09-27	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in the web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049 FP9, 9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before 9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string, a different vulnerability than CVE-2016-5975. **Reference: CVE-2016-5978**	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/107
NA	2016-09-27	4.9	Open redirect vulnerability in the web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/108

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

			FP9, 9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before 9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 allows remote authenticated users to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **Reference: CVE-2016-5977**		
Gain Information	2016-09-27	2.6	The web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049 FP9, 9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before 9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 allows remote authenticated users to discover component passwords via unspecified vectors. **Reference: CVE-2016-5976**	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/109
Cross-site scripting	2016-09-27	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in the web portal in IBM Tealeaf Customer Experience before 8.7.1.8847 FP10, 8.8 before 8.8.0.9049 FP9, 9.0.0 and 9.0.1 before 9.0.1.1117 FP5, 9.0.1A before	http://www-01.ibm.com/support/docview.wss?uid=swg21990216	A-IBM-TEALE-101016/110

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

			9.0.1.5108_9.0.1A FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224_9.0.2A FP3 allows remote authenticated users to inject arbitrary web script or HTML via an embedded string, a different vulnerability than CVE-2016-5978. **Reference: CVE-2016-5975**		
Websphere Application Server *WebSphere Application Server (WAS) is a software product that performs the role of a web application server.*					
Gain Information	2016-10-03	5	IBM WebSphere Application Server (WAS) 7.x before 7.0.0.43, 8.0.x before 8.0.0.13, 8.5.x before 8.5.5.11, 9.0.x before 9.0.0.2, and Liberty before 16.0.0.3 mishandles responses, which allows remote attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-5986**	http://www-01.ibm.com/support/docview.wss?uid=swg21990056	A-IBM-WEBSP-101016/111
Cross-site scripting	2016-10-03	3.5	Cross-site scripting (XSS) vulnerability in the Web UI in IBM WebSphere Application Server (WAS) Liberty before 16.0.0.3 allows remote authenticated users to inject arbitrary web script or HTML via vectors involving OpenID Connect clients. **Reference: CVE-2016-3042**	http://www-01.ibm.com/support/docview.wss?uid=swg21986716	A-IBM-WEBSP-101016/112
Websphere Mq					

Websphere MQ is an IBM standard for program-to-program messaging across multiple platforms.					
Denial of Service	2016-09-26	3.5	IBM WebSphere MQ 7.5 before 7.5.0.7 and 8.0 before 8.0.0.5 mishandles protocol flows, which allows remote authenticated users to cause a denial of service (channel outage) by leveraging queue-manager rights. **Reference: CVE-2016-0379**	http://www-01.ibm.com/support/docview.wss?uid=swg21984565	A-IBM-WEBSP-101016/113
ICU Project					
International Components For Unicode *International Components for Unicode (ICU) is an open source project of mature C/C++ and Java libraries for Unicode support, software internationalization, and software globalization.*					
Denial of Service; Overflow	2016-09-19	7.5	Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long locale string. **Reference: CVE-2016-7415**	NA	A-ICU-INTER-101016/114
ISC					
Bind *BIND is open source software that implements the Domain Name System (DNS) protocols for the Internet.*					
Denial of Service	2016-09-28	7.8	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct	https://kb.isc.org/article/AA-01419/0	A-ISC-BIND-101016/115

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

			responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query. **Reference: CVE-2016-2776**		
Libarchive					
Libarchive *Libarchive is an open-source BSD-licensed C programming library that provides streaming access to a variety of different archive formats, including tar, cpio, pax, Zip, and ISO9660 images.*					
Denial of Service	2016-09-20	4.3	The trad_enc_decrypt_update function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap read and crash) via a crafted zip file, related to reading the password. **Reference: CVE-2015-8927**	NA	A-LIB-LIBAR-101016/116
Denial of Service	2016-09-20	4.3	bsdcpio in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read and crash) via crafted cpio file. **Reference: CVE-2015-8915**	NA	A-LIB-LIBAR-101016/117
Execute Code Overflow	2016-09-21	6.8	Stack-based buffer overflow in the parse_device function in archive_read_support_format_mtree.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a crafted mtree	https://github.com/libarchive/libarchive/issues/715	A-LIB-LIBAR-101016/118

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

			file. **Reference: CVE-2016-4301**		
Libgd					
Libgd *Libgd is a graphics library. It allows your code to quickly draw images complete with lines, arcs, text, multiple colors, cut and paste from other images, and flood fills, and writes out the result as a PNG or JPEG file.*					
Denial of Service; Overflow	2016-09-29	7.5	Integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calls. **Reference: CVE-2016-7568**	https://github.com/php/php-src/commit/c18263e0e0769faee96a5d0ee04b750c442783c6	A-LIB-LIBGD-101016/119
Mariadb; Oracle; Percona					
Mariadb/Mysql/Percona Server *MariaDB surpasses MySQL as a leader in open source database solutions by delivering enterprise-level high availability, scalability and security; MySQL is an open-source relational database management system (RDBMS); Percona Server for MySQL is a free, fully compatible, enhanced, open source drop-in replacement for MySQL that provides superior performance, scalability.*					
Execute Code Bypass	2016-09-30	10	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create	https://jira.mariadb.org/browse/MDEV-10465	A-MAR-MARIA-101016/120

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

			arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. **Reference: CVE-2016-6662**		
Microsoft					
Azure Active Directory Passport *Passport-azure-ad is a collection of Passport Strategies to help you integrate with Azure Active Directory.*					
Bypass	2016-09-30	4.3	The Microsoft Azure Active Directory Passport (aka Passport-Azure-AD) library 1.x before 1.4.6 and 2.x before 2.0.1 for Node.js does not recognize the validateIssuer setting, which allows remote attackers to bypass authentication via a crafted token. **Reference: CVE-2016-7191**	https://github.com/AzureAD/passport-azure-ad/blob/master/SECURITY-NOTICE.MD	A-MIC-AZURE-101016/121
Edge; Internet Explorer *Edge / Internet Explorer are browsers (a browser is an application program that provides a way to look at and interact with all the information on the World Wide Web)*					
Gain Information	2016-09-26	2.6	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to obtain sensitive information via a crafted web site, aka "Microsoft Browser Information Disclosure Vulnerability."	NA	A-MIC-EDGE-101016/122

			Reference: CVE-2016-3351		
Excel; Excel Viewer; Office Compatibility Pack *Microsoft Excel is a spreadsheet developed by Microsoft for Windows, Mac OS X, Android and iOS.*					
Execute Code Overflow ; Memory Corruption	2016-09-26	9.3	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3381. **Reference: CVE-2016-3363**	NA	A-MIC-EXCEL-101016/123
Internet Explorer *Internet Explorer is a discontinued series of graphical web browsers developed by Microsoft and included as part of the Microsoft Windows line of operating.*					
Bypass	2016-09-19	5.1	Microsoft Internet Explorer 9 through 11 mishandles .url files from the Internet zone, which allows remote attackers to bypass intended access restrictions via a crafted file, aka "Internet Explorer Security Feature Bypass." **Reference: CVE-2016-3353**	NA	A-MIC-INTER-101016/124
Mozilla					
Firefox *Mozilla Firefox is a fast, light and tidy open source web browser.*					
Bypass	2016-09-23	6.8	Mozilla Firefox before 49.0 allows remote attackers to bypass the Same Origin Policy via a	https://bugzilla.mozilla.org/show_bug.cgi?id=928187	A-MOZ-FIREF-101016/125

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

			crafted fragment identifier in the SRC attribute of an IFRAME element, leading to insufficient restrictions on link-color information after a document is resized. **Reference: CVE-2016-5283**		
Gain Information	2016-09-23	4.3	Mozilla Firefox before 49.0 does not properly restrict the scheme in favicon requests, which might allow remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by a jar: URL for a favicon resource. **Reference: CVE-2016-5282**	https://bugzilla.mozilla.org/show_bug.cgi?id=932335	A-MOZ-FIREF-101016/126
Gain Information	2016-09-23	4.3	Mozilla Firefox before 49.0 allows user-assisted remote attackers to obtain sensitive full-pathname information during a local-file drag-and-drop operation via crafted JavaScript code. **Reference: CVE-2016-5279**	https://bugzilla.mozilla.org/show_bug.cgi?id=1249522	A-MOZ-FIREF-101016/127
Execute Code Overflow	2016-09-23	6.8	Buffer overflow in the mozilla::gfx::FilterSupport::ComputeSourceNeededRegions function in Mozilla Firefox before 49.0 allows remote attackers to execute arbitrary code by leveraging improper interaction between empty filters and	https://bugzilla.mozilla.org/show_bug.cgi?id=1287316	A-MOZ-FIREF-101016/128

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

			CANVAS element rendering. **Reference: CVE-2016-5275**		
Execute Code	2016-09-23	6.8	The mozilla::a11y::HyperTextAccessible::GetChildOffset function in the accessibility implementation in Mozilla Firefox before 49.0 allows remote attackers to execute arbitrary code via a crafted web site. **Reference: CVE-2016-5273**	https://bugzilla.mozilla.org/show_bug.cgi?id=1280387	A-MOZ-FIREF-101016/129
Denial of Service	2016-09-23	4.3	The PropertyProvider::GetSpacingInternal function in Mozilla Firefox before 49.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via text runs in conjunction with a "display: contents" Cascading Style Sheets (CSS) property. **Reference: CVE-2016-5271**	https://bugzilla.mozilla.org/show_bug.cgi?id=1288946	A-MOZ-FIREF-101016/130
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-23	7.5	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	https://bugzilla.mozilla.org/show_bug.cgi?id=1297099	A-MOZ-FIREF-101016/131

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-2016-5256		
Denial of Service	2016-09-23	4.3	The mozilla::net::IsValidReferrerPolicy function in Mozilla Firefox before 49.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a Content Security Policy (CSP) referrer directive with zero values. **Reference: CVE-2016-2827**	https://bugzilla.mozilla.org/show_bug.cgi?id=1289085	A-MOZ-FIREF-101016/132
Firefox;Firefox Esr *Mozilla Firefox is a fast, light and tidy open source web browser; Firefox ESR is intended for groups who deploy and maintain the desktop.*					
NA	2016-09-23	4.3	Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 rely on unintended expiration dates for Preloaded Public Key Pinning, which allows man-in-the-middle attackers to spoof add-on updates by leveraging possession of an X.509 server certificate for addons.mozilla.org signed by an arbitrary built-in Certification Authority. **Reference: CVE-2016-5284**	http://www.mozilla.org/security/announce/2016/mfsa2016-85.html	A-MOZ-FIREF-101016/133
Execute Code	2016-09-23	7.5	Use-after-free vulnerability in the DOMSVGLength class in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code	https://bugzilla.mozilla.org/show_bug.cgi?id=1284690	A-MOZ-FIREF-101016/134

			by leveraging improper interaction between JavaScript code and an SVG document. **Reference: CVE-2016-5281**		
Execute Code	2016-09-23	7.5	Use-after-free vulnerability in the mozilla::nsTextNodeDirectionalityMap::RemoveElementFromMap function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code via bidirectional text. **Reference: CVE-2016-5280**	https://bugzilla.mozilla.org/show_bug.cgi?id=1289970	A-MOZ-FIREF-101016/135
Execute Code Overflow	2016-09-23	6.8	Heap-based buffer overflow in the nsBMPEncoder::AddImageFrame function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code via a crafted image data that is mishandled during the encoding of an image frame to an image. **Reference: CVE-2016-5278**	https://bugzilla.mozilla.org/show_bug.cgi?id=1294677	A-MOZ-FIREF-101016/136
Denial of Service; Execute Code ;Memory Corruption	2016-09-23	7.5	Use-after-free vulnerability in the nsRefreshDriver::Tick function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code or cause	https://bugzilla.mozilla.org/show_bug.cgi?id=1291665	A-MOZ-FIREF-101016/137

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

			a denial of service (heap memory corruption) by leveraging improper interaction between timeline destruction and the Web Animations model implementation. **Reference: CVE-2016-5277**		
Denial of Service; Execute Code ;Memory Corruption	2016-09-23	7.5	Use-after-free vulnerability in the mozilla::a11y::DocAccessible::ProcessInvalidationList function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an aria-owns attribute. **Reference: CVE-2016-5276**	https://bugzilla.mozilla.org/show_bug.cgi?id=1287721	A-MOZ-FIREF-101016/138
Execute Code	2016-09-23	7.5	Use-after-free vulnerability in the nsFrameManager::CaptureFrameState function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between restyling and the Web Animations model implementation. **Reference: CVE-2016-5274**	https://bugzilla.mozilla.org/show_bug.cgi?id=1282076	A-MOZ-FIREF-101016/139
Execute Code	2016-09-23	6.8	The nsImageGeometryMixin class in Mozilla Firefox	https://bugzilla.mozilla.org/show_bug.cgi?id=12	A-MOZ-FIREF-101016/140

			before 49.0 and Firefox ESR 45.x before 45.4 does not properly perform a cast of an unspecified variable during handling of INPUT elements, which allows remote attackers to execute arbitrary code via a crafted web site. **Reference: CVE-2016-5272**	97934	
Denial of Service; Overflow	2016-09-23	7.5	Heap-based buffer overflow in the nsCaseTransformTextRunFactory::TransformString function in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allows remote attackers to cause a denial of service (boolean out-of-bounds write) or possibly have unspecified other impact via Unicode characters that are mishandled during text conversion. **Reference: CVE-2016-5270**	https://bugzilla.mozilla.org/show_bug.cgi?id=1291016	A-MOZ-FIREF-101016/141
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-23	7.5	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 and Firefox ESR 45.x before 45.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.	https://bugzilla.mozilla.org/show_bug.cgi?id=1294407	A-MOZ-FIREF-101016/142

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-2016-5257		
Nextcloud/Owncloud					
Nextcloud/Owncloud *Nextcloud, the next generation Enterprise File Sync & Share was started by ownCloud inventor Frank Karlitschek to empower users to take back control over their data and communication; OwnCloud is an open source, self-hosted file sync and share app platform. Access & sync your files, contacts, calendars & bookmarks across your devices.*					
Cross-site scripting	2016-09-19	3.5	Cross-site scripting (XSS) vulnerability in share.js in the gallery application in ownCloud Server before 9.0.4 and Nextcloud Server before 9.0.52 allows remote authenticated users to inject arbitrary web script or HTML via a crafted directory name. **Reference: CVE-2016-7419**	https://owncloud.org/security/advisory/?id=oc-sa-2016-011	A-NEX-NEXTC-101016/143
Opendental					
Opendental *Open Dental, previously known as Free Dental, is Practice Management Software licensed under the GNU General Public License.*					
NA	2016-09-28	7.5	** DISPUTED ** Open Dental 16.1 and earlier has a hardcoded MySQL root password, which allows remote attackers to obtain administrative access by leveraging access to intranet TCP port 3306. NOTE: the vendor disputes this issue, stating that the "vulnerability note ... is factually false ... there is indeed a default blank password, but it can be changed ... We recommend that users change it, each	NA	A-OPE-OPEND-101016/144

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

			customer receives direction." **Reference: CVE-2016-6531**		
Openssl					
Openssl *In computer networking, OpenSSL is a software library to be used in applications that need to secure communications against eavesdropping or need to ascertain the identity*					
Denial of Service; Overflow	2016-09-16	7.5	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors. **Reference: CVE-2016-6303**	https://bugzilla.redhat.com/show_bug.cgi?id=1370146	A-OPE-OPENS-101016/145
Denial of Service	2016-09-16	5	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short. **Reference: CVE-2016-6302**	https://git.openssl.org/?p=openssl.git;a=commit;h=e97763c92c655dcf4af2860b3abd2bc4c8a267f9	A-OPE-OPENS-101016/146
Denial of Service	2016-09-16	7.5	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote	https://git.openssl.org/?p=openssl.git;a=commit;h=07bed46f332fce8c1d157689a2cdf915a982ae34	A-OPE-OPENS-101016/147

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

			attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors. **Reference: CVE-2016-2182**		
Denial of Service	2016-09-16	5	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c. **Reference: CVE-2016-2181**	https://git.openssl.org/?p=openssl.git;a=commit;h=1fb9fdc3027b27d8eb6a1e6a846435b070980770	A-OPE-OPENS-101016/148
Denial of Service	2016-09-16	5	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c,	https://git.openssl.org/?p=openssl.git;a=commit;h=f5c7f5dfbaf0d2f7d946d0fe86f08e6bcb36ed0d	A-OPE-OPENS-101016/149

			statem_lib.c, and statem_srvr.c. **Reference: CVE-2016-2179**		
Denial of Service; Execute Code	2016-09-27	10	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote attackers to cause a denial of service (use-after-free) or possibly execute arbitrary code via a crafted TLS session. **Reference: CVE-2016-6309**	https://www.openssl.org/news/secadv/20160926.txt	A-OPE-OPENS-101016/150
Denial of Service	2016-09-27	7.1	statem/statem_dtls.c in the DTLS implementation in OpenSSL 1.1.0 before 1.1.0a allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted DTLS messages. **Reference: CVE-2016-6308**	https://www.openssl.org/news/secadv/20160922.txt	A-OPE-OPENS-101016/151
Denial of Service	2016-09-27	4.3	The state-machine implementation in OpenSSL 1.1.0 before 1.1.0a allocates memory before checking for an excessive length, which might allow remote attackers to cause a denial of service (memory consumption) via crafted TLS messages, related to statem/statem.c and	https://www.openssl.org/news/secadv/20160922.txt	A-OPE-OPENS-101016/152

			statem/statem_lib.c. **Reference: CVE-2016-6307**		
Denial of Service	2016-09-27	4.3	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c. **Reference: CVE-2016-6306**	https://www.openssl.org/news/secadv/20160922.txt	A-OPE-OPENS-101016/153
Denial of Service	2016-09-27	5	The ssl3_read_bytes function in record/rec_layer_s3.c in OpenSSL 1.1.0 before 1.1.0a allows remote attackers to cause a denial of service (infinite loop) by triggering a zero-length record in an SSL_peek call. **Reference: CVE-2016-6305**	https://www.openssl.org/news/secadv/20160922.txt	A-OPE-OPENS-101016/154
Denial of Service	2016-09-27	7.8	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions. **Reference: CVE-2016-6304**	https://www.openssl.org/news/secadv/20160922.txt	A-OPE-OPENS-101016/155
Denial of Service	2016-09-30	5	crypto/x509/x509_vfy.c in OpenSSL 1.0.2i allows remote attackers to cause a denial of service (NULL pointer	https://www.openssl.org/news/secadv/20160926.txt	A-OPE-OPENS-101016/156

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

			dereference and application crash) by triggering a CRL operation. **Reference: CVE-2016-7052**		
Openstack					
Compute (nova) *Nova is an OpenStack component that provides on-demand access to compute resources by provisioning and managing large networks of virtual machines.*					
Denial of Service	2016-09-28	6.8	OpenStack Compute (nova) 13.0.0 does not properly delete instances from compute nodes, which allows remote authenticated users to cause a denial of service (disk consumption) by deleting instances while in the resize state. NOTE: this vulnerability exists because of a CVE-2015-3280 regression. **Reference: CVE-2016-7498**	https://security.openstack.org/ossa/OSSA-2016-011.html	A-OPE-COMPU-101016/157
Mitaka-murano; Murano; Murano-dashboard; Python-muranoclient *Murano Project introduces an application catalog to OpenStack, enabling application developers and cloud administrators to publish various cloud-ready applications in a browsable categorized catalog; Murano-dashboard Murano UI implemented as a plugin for OpenStack Dashboard; Python-muranoclient Client library and CLI client for Murano.*					
Execute Code	2016-09-28	7.5	OpenStack Murano before 1.0.3 (liberty) and 2.x before 2.0.1 (mitaka), Murano-dashboard before 1.0.3 (liberty) and 2.x before 2.0.1 (mitaka), and python-muranoclient before 0.7.3 (liberty) and 0.8.x before 0.8.5 (mitaka) improperly use loaders inherited from yaml.Loader when	https://bugs.launchpad.net/murano/+bug/1586079	A-OPE-MITAK-101016/158

			parsing MuranoPL and UI files, which allows remote attackers to create arbitrary Python objects and execute arbitrary code via crafted extended YAML tags in UI definitions in packages. **Reference: CVE-2016-4972**		
Oracle					
Linux *The Linux operating system is based on it and deployed on both traditional computer systems such as personal computers and servers, usually in the form of Linux distributions.*					
NA	2016-09-30	4.6	Unspecified vulnerability in the kernel-uek component in Oracle Linux 6 allows local users to affect availability via unknown vectors. **Reference: CVE-2016-0617**	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html	A-ORA-LINUX-101016/159
Otrs					
FAQ *OTRS also has a public web interface which is available through the FAQ-Module.*					
Execute Code; Sql Injection	2016-09-19	9	Multiple SQL injection vulnerabilities in the FAQ package 2.x before 2.3.6, 4.x before 4.0.5, and 5.x before 5.0.5 in Open Ticket Request System (OTRS) allow remote attackers to execute arbitrary SQL commands via crafted search parameters. **Reference: CVE-2016-5843**	https://www.otrs.com/security-advisory-2016-01-security-update-otrs-faq-package/	A-OTR-FAQ-101016/160
PHP					
PHP *PHP is a general-purpose scripting language that is especially suited to server-side web development, in which case PHP generally runs on a web server.*					

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	2016-09-19	5	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call. **Reference: CVE-2016-7418**	https://github.com/php/php-src/commit/c4cca4c20e75359c9a13a1f9a36cb7b4e9601d29?w=1	A-PHP-PHP-101016/161
Denial of Service	2016-09-19	7.5	ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data. **Reference: CVE-2016-7417**	https://github.com/php/php-src/commit/ecb7f58a069be0dec4a6131b6351a761f808f22e?w=1	A-PHP-PHP-101016/162
Denial of Service; Overflow	2016-09-19	5	ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers	https://github.com/php/php-src/commit/6d55ba265637d6adf0ba7e9c9ef11187d1ec2f5b?w=1	A-PHP-PHP-101016/163

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

			to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument. **Reference: CVE-2016-7416**		
Denial of Service; Overflow	2016-09-19	7.5	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c. **Reference: CVE-2016-7414**	https://github.com/php/php-src/commit/0bfb970f43acd1e81d11be1154805f86655f15d5?w=1	A-PHP-PHP-101016/164
Denial of Service	2016-09-19	7.5	Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to	https://github.com/php/php-src/commit/b88393f08a558eec14964a55d3c680fe67407712?w=1	A-PHP-PHP-101016/165

			mishandling in a wddx_deserialize call. **Reference: CVE-2016-7413**		
Denial of Service; Overflow	2016-09-19	6.8	ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata. **Reference: CVE-2016-7412**	https://github.com/php/php-src/commit/28f80baf3c53e267c9ce46a2a0fadbb981585132?w=1	A-PHP-PHP-101016/166
Denial of Service; Overflow ;Memory Corruption	2016-09-19	7.5	ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object. **Reference: CVE-2016-7411**	https://github.com/php/php-src/commit/6a7cc8ff85827fa9ac715b3a83c2d9147f33cd43?w=1	A-PHP-PHP-101016/167
Pivotal					
Cloud Foundry Elastic Runtime *Cloud Foundry is an open source cloud computing platform as a service.*					
NA	2016-09-19	5.8	Multiple open redirect vulnerabilities in Pivotal Cloud Foundry (PCF) Elastic Runtime	https://pivotal.io/security/cve-2016-0928	A-PIV-CLOUD-101016/168

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

			before 1.6.30 and 1.7.x before 1.7.8 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors. **Reference: CVE-2016-0928**		
Cross-site scripting	2016-09-19	4.3	Cross-site scripting (XSS) vulnerability in Apps Manager in Pivotal Cloud Foundry (PCF) Elastic Runtime before 1.6.32 and 1.7.x before 1.7.8 allows remote attackers to inject arbitrary web script or HTML via unspecified input that improperly interacts with the AngularJS framework. **Reference: CVE-2016-0926**	https://pivotal.io/security/cve-2016-0926	A-PIV-CLOUD-101016/169
Operations Manager *Operations Manager is a web application that you use to deploy and manage a Pivotal Cloud Foundry (PCF) PaaS.*					
NA	2016-09-20	5	Pivotal Cloud Foundry (PCF) Ops Manager before 1.6.19 and 1.7.x before 1.7.10, when vCloud or vSphere is used, has a default password for compilation VMs, which allows remote attackers to obtain SSH access by connecting within an installation-time period during which these VMs exist. **Reference: CVE-2016-0930**	https://pivotal.io/security/cve-2016-0930	A-PIV-OPERA-101016/170
Cross-site	2016-09-30	4.3	Cross-site scripting	https://pivotal.i	A-PIV-

scripting			(XSS) vulnerability in Pivotal Cloud Foundry (PCF) Ops Manager before 1.6.17 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-0927**	o/security/cve-2016-0927	CLOUD-101016/171
Cloud Foundry Elastic Runtime *Cloud Foundry gives companies the speed, simplicity and control they need to develop and deploy applications faster and easier*					
Bypass	2016-09-30	7.5	Pivotal Cloud Foundry (PCF) Elastic Runtime before 1.6.34 and 1.7.x before 1.7.12 places 169.254.0.0/16 in the all_open Application Security Group, which might allow remote attackers to bypass intended network-connectivity restrictions by leveraging access to the 169.254.169.254 address. **Reference: CVE-2016-0896**	https://pivotal.io/security/cve-2016-0896	A-PIV-CLOUD-101016/172
Cloud Foundry;Cloud Foundry Elastic Runtime; Cloud Foundry Ops Manager; Cloud Foundry Uaa; Cloud Foundry Uaa Bosh: *Cloud Foundry gives companies the speed, simplicity and control they need to develop and deploy applications faster and easier; Operations Manager is a web application that you use to deploy and manage a Pivotal Cloud Foundry (PCF) PaaS; User Account and Authentication Service (UAA) in Cloud Foundry is responsible for securing the platform services and providing a single sign on for web applications.*					
Gain Privileges	2016-09-30	6.5	The UAA /oauth/token endpoint in Pivotal Cloud Foundry (PCF) before 243; UAA 2.x before 2.7.4.8, 3.x before 3.3.0.6, and 3.4.x before 3.4.5; UAA BOSH before 11.7 and 12.x	https://pivotal.io/security/cve-2016-6651	A-PIV-CLOUD-101016/173

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

			before 12.6; Elastic Runtime before 1.6.40, 1.7.x before 1.7.21, and 1.8.x before 1.8.2; and Ops Manager 1.7.x before 1.7.13 and 1.8.x before 1.8.1 allows remote authenticated users to gain privileges by leveraging possession of a token. **Reference: CVE-2016-6651**		
Cross Site Request Forgery	2016-09-30	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in Pivotal Cloud Foundry (PCF) before 242; UAA 2.x before 2.7.4.7, 3.x before 3.3.0.5, and 3.4.x before 3.4.4; UAA BOSH before 11.5 and 12.x before 12.5; Elastic Runtime before 1.6.40, 1.7.x before 1.7.21, and 1.8.x before 1.8.2; and Ops Manager 1.7.x before 1.7.13 and 1.8.x before 1.8.1 allow remote attackers to hijack the authentication of unspecified victims for requests that approve or deny a scope via a profile or authorize approval page. **Reference: CVE-2016-6637**	https://pivotal.io/security/cve-2016-6637	A-PIV-CLOUD-101016/174
NA	2016-09-30	5	The OAuth authorization implementation in Pivotal Cloud Foundry (PCF) before 242; UAA 2.x before 2.7.4.7, 3.x	https://pivotal.io/security/cve-2016-6636	A-PIV-CLOUD-101016/175

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

			before 3.3.0.5, and 3.4.x before 3.4.4; UAA BOSH before 11.5 and 12.x before 12.5; Elastic Runtime before 1.6.40, 1.7.x before 1.7.21, and 1.8.x before 1.8.1; and Ops Manager 1.7.x before 1.7.13 and 1.8.x before 1.8.1 mishandles redirect_uri subdomains, which allows remote attackers to obtain implicit access tokens via a modified subdomain. **Reference: CVE-2016-6636**		
Operations Manager *Pivotal CF is the first integrated platform encompassing the industry's leading big data framework, Apache Hadoop, and the leading open source PaaS, Cloud Foundry, to enable enterprise developers and cloud operators to build, manage and scale a new class of applications that leverage modern frameworks that instantly bind to massive data sets.*					
NA	2016-10-03	7.5	Pivotal Cloud Foundry (PCF) Ops Manager before 1.6.17 and 1.7.x before 1.7.8, when vCloud or vSphere is used, does not properly enable SSH access for operators, which has unspecified impact and remote attack vectors. **Reference: CVE-2016-0897**	https://pivotal.io/security/cve-2016-0897	A-PIV-OPERA-101016/176
Bypass	2016-10-03	5	Pivotal Cloud Foundry (PCF) Ops Manager before 1.5.14 and 1.6.x before 1.6.9 uses the same cookie-encryption key across different customers' installations, which allows remote attackers to bypass session authentication	https://pivotal.io/security/pcf-ops-manager-weak-authentication-scheme	A-PIV-OPERA-101016/177

			by leveraging knowledge of this key from another installation. **Reference: CVE-2016-0883**		
Rabbitmq *RabbitMQ offers a variety of features to let you trade off performance with reliability, including persistence, delivery acknowledgements, publisher confirms, and high availability.Pivotal provides a full range of commercial support and services for RabbitMQ.*					
Gain Information	2016-10-03	5	The metrics-collection component in RabbitMQ for Pivotal Cloud Foundry (PCF) 1.6.x before 1.6.4 logs command lines of failed commands, which might allow context-dependent attackers to obtain sensitive information by reading the log data, as demonstrated by a syslog message that contains credentials from a command line. **Reference: CVE-2016-0929**	https://pivotal.io/security/cve-2016-0929	A-PIV-RABBI-101016/178
Powerdns					
Authoritative *The PowerDNS Authoritative Server is the only solution that enables authoritative DNS service from all major databases, including but not limited to MySQL, PostgreSQL, SQLite3, Oracle, Sybase, Microsoft SQL Server, LDAP and plain text files.*					
Denial of Service	2016-09-21	5	PowerDNS (aka pdns) Authoritative Server before 3.4.10 does not properly handle a . (dot) inside labels, which allows remote attackers to cause a denial of service (backend CPU consumption) via a crafted DNS query.	https://github.com/PowerDNS/pdns/commit/881b5b03a590198d03008e4200dd00cc537712f3	A-POW-AUTHO-101016/179

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-2016-5427		
Denial of Service	2016-09-21	5	PowerDNS (aka pdns) Authoritative Server before 3.4.10 allows remote attackers to cause a denial of service (backend CPU consumption) via a long qname. **Reference: CVE-2016-5426**	https://github.com/PowerDNS/pdns/commit/881b5b03a590198d03008e4200dd00cc537712f3	A-POW-AUTHO-101016/180
Python					
Python *Python is an easy to learn, powerful programming language. It has efficient high level data structures and a simple but effective approach to object-oriented.*					
NA	2016-09-22	4.3	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL. **Reference: CVE-2016-5699**	http://www.oracle.com/technetwork/topics/security/bulletinjul2016-3090568.html	A-PYT-PYTHO-101016/181
Overflow	2016-09-22	10	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow. **Reference: CVE-2016-5636**	https://hg.python.org/cpython/raw-file/v2.7.12/Misc/NEWS	A-PYT-PYTHO-101016/182

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

Redhat					
Jboss Enterprise Application Platform *JBoss Enterprise Application Platform (or JBoss EAP) is a subscription-based/open-source Java EE-based application server runtime platform used for building, deploying, and hosting highly-transactional Java applications and services.*					
Gain Privileges	2016-09-28	6.5	The domain controller in Red Hat JBoss Enterprise Application Platform (EAP) 7.x before 7.0.2 allows remote authenticated users to gain privileges by leveraging failure to propagate administrative RBAC configuration to all slaves. **Reference: CVE-2016-5406**	https://bugzilla.redhat.com/show_bug.cgi?id=1359014	A-RED-JBOSS-101016/183
Jboss Enterprise Application Platform;Jboss Wildfly Application Server *JBoss Enterprise Application Platform (or JBoss EAP) is a subscription-based/open-source Java EE-based application server runtime platform used for building, deploying, and hosting highly-transactional Java applications and services; WildFly is a flexible, lightweight, managed application runtime that helps you build amazing applications.*					
Http R.Spl.	2016-09-29	4.3	CRLF injection vulnerability in the Undertow web server in WildFly 10.0.0, as used in Red Hat JBoss Enterprise Application Platform (EAP) 7.x before 7.0.2, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors. **Reference: CVE-2016-4993**	https://bugzilla.redhat.com/show_bug.cgi?id=1344321	A-RED-JBOSS-101016/184
Jboss Enterprise Web Server *JBoss Enterprise Web Server removes the complexity from managing open source-based web application environments.*					
Denial of	2016-09-27	5	mod_cluster, as used in	https://bugzilla.	A-RED-

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

Service			Red Hat JBoss Web Server 2.1, allows remote attackers to cause a denial of service (Apache http server crash) via an MCMP message containing a series of = (equals) characters after a legitimate element. **Reference: CVE-2016-3110**	redhat.com/show_bug.cgi?id=1326320	JBOSS-101016/185
Jboss Operations Network *JBoss Operations Network simplifies developing, testing, deploying and monitoring your JBoss solutions and the applications running on it.*					
Execute Code	2016-09-28	9	The server in Red Hat JBoss Operations Network (JON), when SSL authentication is not configured for JON server / agent communication, allows remote attackers to execute arbitrary code via a crafted HTTP request, related to message deserialization. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-3737. **Reference: CVE-2016-6330**	https://bugzilla.redhat.com/show_bug.cgi?id=1368864	A-RED-JBOSS-101016/186
Quickstart Cloud Installer *The QuickStart Cloud Installer (QCI) provides a web-based graphical user interface to provision cloud products.*					
NA	2016-09-22	2.1	The kickstart file in Red Hat QuickStart Cloud Installer (QCI) forces use of MD5 passwords on deployed systems, which makes it easier for attackers to determine cleartext	https://bugzilla.redhat.com/show_bug.cgi?id=1370315	A-RED-QUICK-101016/187

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

			passwords via a brute-force attack. **Reference: CVE-2016-6340**		
NA	2016-09-22	7.2	Red Hat QuickStart Cloud Installer (QCI) uses world-readable permissions for /etc/qci/answers, which allows local users to obtain the root password for the deployed system by reading the file. **Reference: CVE-2016-6322**	https://bugzilla.redhat.com/show_bug.cgi?id=1366413	A-RED-QUICK-101016/188
Rockwellautomation					
Rslogix 500 Professional Edition;Rslogix 500 Standard Edition;Rslogix 500 Starter Edition;Rslogix Micro Developer;Rslogix Micro Starter Lite *The RSLogix family of logic programming packages helps you maximize performance, save project development time, and improve productivity.*					
Execute Code Overflow	2016-09-20	9.3	Buffer overflow in Rockwell Automation RSLogix Micro Starter Lite, RSLogix Micro Developer, RSLogix 500 Starter Edition, RSLogix 500 Standard Edition, and RSLogix 500 Professional Edition allows remote attackers to execute arbitrary code via a crafted RSS project file. **Reference: CVE-2016-5814**	https://ics-cert.us-cert.gov/advisories/ICSA-16-224-02	A-ROC-RSLOG-101016/189
SAP					
Hana *SAP HANA is an in-memory, column-oriented, relational database management system developed and marketed by SAPSE.*					
NA	2016-09-28	5	SAP HANA DB 1.00.73.00.389160 (NewDB100_REL) allows remote attackers	NA	A-SAP-HANA-101016/190

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

			to inject arbitrary audit trail fields into the SYSLOG via vectors related to the SQL protocol, aka SAP Security Note 2197459. **Reference: CVE-2016-6142**		
Hana Db *SAP HANA is an in-memory, column-oriented, relational database management system developed and marketed by SAP SE.*					
Gain Information	2016-09-28	5	SAP HANA DB 1.00.091.00.1418659308 allows remote attackers to obtain sensitive topology information via an unspecified HTTP request, aka SAP Security Note 2176128. **Reference: CVE-2016-3639**	NA	A-SAP-HANA-101016/191
Trex *The TREX engine is a standalone component that can be used in a range of system environments but is used primarily as an integral part of such SAP products as Enterprise Portal, Knowledge Warehouse, and Business Intelligence (BI, formerly SAP Business Information Warehouse).*					
Gain Information	2016-09-28	5	The NameServer in SAP TREX 7.10 Revision 63 allows remote attackers to obtain sensitive TNS information via an unspecified query, aka SAP Security Note 2234226. **Reference: CVE-2016-6146**	NA	A-SAP-TREX-101016/192
Execute Code	2016-09-28	10	An unspecified function in SAP TREX 7.10 Revision 63 allows remote attackers to execute arbitrary OS commands via unknown vectors, aka SAP Security Note	NA	A-SAP-TREX-101016/193

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-2016-6137**		
Trane					
Tracer Sc *The Tracer SC is an intelligent field panel that communicates with unit controllers that provide standalone control of HVAC equipment.*					
Gain Privileges	2016-09-19	6.9	ABB DataManagerPro 1.x before 1.7.1 allows local users to gain privileges by replacing a DLL file in the package directory. **Reference: CVE-2016-4526**	https://library.e.abb.com/public/93e52dbfd6ab4f64aa435973ccf1b6e2/9ADB005557_ABB_SoftwareVulnerabilityHandlingAdvisory_DMPro.pdf	A-TRA-TRACE-101016/194
Gain Information	2016-09-19	5	The web server in Trane Tracer SC 4.2.1134 and earlier allows remote attackers to read sensitive configuration files via a direct request. **Reference: CVE-2016-0870**	https://ics-cert.us-cert.gov/advisories/ICSA-16-259-03	A-TRA-TRACE-101016/195
Wireshark					
Wireshark *Wireshark is a network protocol analyzer for Unix and Windows.*					
Denial of Service	2016-09-30	4.3	epan/dissectors/packet-qnet6.c in the QNX6 QNET dissector in Wireshark 2.x before 2.0.6 mishandles MAC address data, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted packet. **Reference: CVE-2016-7175**	https://code.wireshark.org/review/16965	A-WIR-WIRES-101016/196
Yokogawa					
Stardom Fcn/fcj					

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

Stardom Fcn/fcj is a logic designer.					
Denial of Service	2016-09-20	7.5	Yokogawa STARDOM FCN/FCJ controller R1.01 through R4.01 does not require authentication for Logic Designer connections, which allows remote attackers to reconfigure the device or cause a denial of service via a (1) stop application program, (2) change value, or (3) modify application command. **Reference: CVE-2016-4860**	https://web-material3.yokogawa.com/YSAR-16-0002-E.pdf	A-YOK-STARD-101016/197
Application; Operating System (A/OS)					
Apache					
Jackrabbit/Debian Linux *Jackrabbit is an open source content repository for the Java platform; Debian systems currently use the Linux kernel or the FreeBSD kernel*					
Cross Site Request Forgery	2016-09-30	6.8	Cross-site request forgery (CSRF) vulnerability in the CSRF content-type check in Jackrabbit-Webdav in Apache Jackrabbit 2.4.x before 2.4.6, 2.6.x before 2.6.6, 2.8.x before 2.8.3, 2.10.x before 2.10.4, 2.12.x before 2.12.4, and 2.13.x before 2.13.3 allows remote attackers to hijack the authentication of unspecified victims for requests that create a resource via an HTTP POST request with a (1) missing or (2) crafted Content-Type header. **Reference: CVE-2016-**	https://issues.apache.org/jira/browse/JCR-4009	A-OS-APA-JACKR-101016/198

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

			6801		
Apple					
Apple Tv;Iphone Os/Itunes;Safari *Apple TV is a digital media player and a microconsole developed and sold by Apple Inc.;iPhone OS is a mobile operating system created and developed by Apple Inc/ Itunes is a mobile application; Safari is a web browser.*					
Execute Code	2016-09-26	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 mishandles error prototypes, which allows remote attackers to execute arbitrary code via a crafted web site. **Reference: CVE-2016-4728**	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/199
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4766, and CVE-2016-4767. **Reference: CVE-2016-4768**	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/200
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption)	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/201

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

			via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4766, and CVE-2016-4768. **Reference: CVE-2016-4767**		
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4767, and CVE-2016-4768. **Reference: CVE-2016-4766**	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/202
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4766, CVE-2016-4767, and CVE-2016-4768. **Reference: CVE-2016-4765**	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/203
Denial of Service; Execute Code	2016-09-27	6.8	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1	https://support.apple.com/HT207158	A- OS-APP-APPLE-101016/204

Overflow ;Memory Corruption			on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4765, CVE-2016-4766, CVE-2016-4767, and CVE-2016-4768. **Reference: CVE-2016-4759**		
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4735. **Reference: CVE-2016-4734**	https://support.apple.com/HT207142	A- OS-APP-APPLE-101016/205
Denial of Service; Execute Code; Overflow ;Memory Corruption	2016-09-26	9.3	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4734, and CVE-2016-4735. **Reference: CVE-2016-**	https://support.apple.com/HT207142	A- OS-APP-APPLE-101016/206

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

			4733		
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-26	6.8	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4730, CVE-2016-4733, CVE-2016-4734, and CVE-2016-4735. **Reference: CVE-2016-4611**	https://support.apple.com/HT207157	A- OS-APP-APPLE-101016/207
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4734. **Reference: CVE-2016-4735**	https://support.apple.com/HT207142	A- OS-APP-APPLE-101016/208
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611,	https://support.apple.com/HT207142	A- OS-APP-APPLE-101016/209

			CVE-2016-4733, CVE-2016-4734, and CVE-2016-4735. **Reference: CVE-2016-4730**		
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	WebKit in Apple iOS before 10, Safari before 10, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4737**	https://support.apple.com/HT207157	A- OS-APP-APPLE-101016/210
Icloud; Itunes; Safari/Iphone Os *Icloud and Itunes are Apple Applications; Safari browser is an application program that provides a way to look at and interact with all the information on the World Wide Web; Iphone OS is the Operating System of iPhone.*					
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	6.8	WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, iCloud before 6.0 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4762**	https://support.apple.com/HT207158	A- OS-APP-ICLOU-101016/211
Gain Information	2016-09-27	4.9	WKWebView in WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 does not properly verify X.509 certificates from HTTPS servers, which allows man-in-the-middle attackers to spoof	https://support.apple.com/HT207143	A- OS-APP-IPHON-101016/212

			servers and obtain sensitive information via a crafted certificate. **Reference: CVE-2016-4763**		
Iphone Os/Itunes; Safari *A media player by Apple Computer that is used for playing digital music or video files; Safari browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.*					
NA	2016-09-27	4.3	WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to conduct DNS rebinding attacks against non-HTTP Safari sessions by leveraging HTTP/0.9 support. **Reference: CVE-2016-4760**	https://support.apple.com/HT207143	A- OS-APP-IPHON-101016/213
Gain Information	2016-09-27	4.3	WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 does not properly restrict access to the location variable, which allows remote attackers to obtain sensitive information via a crafted web site. **Reference: CVE-2016-4758**	https://support.apple.com/HT207157	A- OS-APP-IPHON-101016/214
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	WebKit in Apple iOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4731. **Reference: CVE-2016-**	https://support.apple.com/HT207157	A- OS-APP-IPHON-101016/215

			4729		
Cross-site scripting	2016-09-26	4.3	Cross-site scripting (XSS) vulnerability in Safari Reader in Apple iOS before 10 and Safari before 10 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)." **Reference: CVE-2016-4618**	https://support.apple.com/HT207157	A- OS-APP-IPHON-101016/216
Iphone Os/Safari *iPhone OS is a mobile operating system created and developed by Apple Inc; Safari a browser is an application program that provides a way to look at and interact with all the information on the World Wide Web.*					
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	WebKit in Apple iOS before 10 and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4729. **Reference: CVE-2016-4731**	https://support.apple.com/HT207157	A- OS-APP-IPHON-101016/217
Mupdf/Debian Linux *The renderer in MuPDF is tailored for high quality anti-aliased graphics; Debian is a Unix-like computer operating system.*					
Denial of Service; Execute Code Overflow	2016-09-22	7.5	Heap-based buffer overflow in the pdf_load_mesh_params function in pdf/pdf-shade.c in MuPDF allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a large decode array. **Reference: CVE-2016-6525**	http://git.ghostscript.com/?p=mupdf.git;h=39b0f07dd960f34e7e6bf230ffc3d87c41ef0f2e	A- OS-ART-MUPDF-101016/218

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

Mupdf/ Leap; Opensuse *The renderer in MuPDF is tailored for high quality anti-aliased graphics; LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution; The openSUSE project is a worldwide effort that promotes the use of Linux/ Eye of Genome is the official image viewer for the Gnome desktop environment.*					
Denial of Service	2016-09-22	4.3	Use-after-free vulnerability in the pdf_load_xref function in pdf/pdf-xref.c in MuPDF allows remote attackers to cause a denial of service (crash) via a crafted PDF file. **Reference: CVE-2016-6265**	http://git.ghostscript.com/?p=mupdf.git;h=fa1936405b6a84e5c9bb440912c23d532772f958	A- OS-ART-MUPDF-101016/219
Canonical					
Ubuntu Linux/File Roller *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers; File-roller is an archive manager for the GNOME environment*					
NA	2016-09-28	5	The _g_file_remove_directory function in file-utils.c in File Roller 3.5.4 through 3.20.2 allows remote attackers to delete arbitrary files via a symlink attack on a folder in an archive. **Reference: CVE-2016-7162**	https://git.gnome.org/browse/file-roller/commit/?id=f70be1f41688859ec8dbe266df35a1839ceb96c5	A- OS-CAN-UBUNT-101016/220
Ubuntu Linux/Debian Linux/Irssi *Linux is an open-source operating system modelled on UNIX; Irssi is an IRC client program for Linux, FreeBSD, Mac OS X and Microsoft Windows.*					
Denial of Service; Overflow	2016-09-28	5	The format_send_to_gui function in the format parsing code in Irssi before 0.8.20 allows remote attackers to cause a denial of service (heap corruption and crash) via vectors involving the length of a string. **Reference: CVE-2016-7045**	https://irssi.org/security/irssi_sa_2016.txt	A- OS-CAN-UBUNT-101016/221

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	2016-09-28	5	The unformat_24bit_color function in the format parsing code in Irssi before 0.8.20, when compiled with true-color enabled, allows remote attackers to cause a denial of service (heap corruption and crash) via an incomplete 24bit color code. **Reference: CVE-2016-7044**	https://irssi.org/security/irssi_sa_2016.txt	A- OS-CAN-UBUNT-101016/222
Ubuntu Linux/Debian Linux/Libarchive *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers; Libarchive is an open-source BSD-licensed C programming library that provides streaming access to a variety of different archive formats, including tar, cpio, pax, Zip, and ISO9660 images.*					
Denial of Service	2016-09-27	5	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an invalid character in the name of a cab file. **Reference: CVE-2015-8917**	https://security-tracker.debian.org/tracker/CVE-2015-8917	A- OS-CAN-UBUNT-101016/223
Denial of Service	2016-09-27	4.3	bsdtar in libarchive before 3.2.0 returns a success code without filling the entry when the header is a "split file in multivolume RAR," which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted rar file. **Reference: CVE-2015-8916**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/224
Ubuntu Linux/Debian Linux/Linux Enterprise Desktop; Linux Enterprise Server; Linux Enterprise Software Development Kit/Libarchive *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers; Libarchive is an open-source BSD-licensed C programming library*					

that provides streaming access to a variety of different archive formats, including tar, cpio, pax, Zip, and ISO9660 images.					
Denial of Service	2016-09-27	4.3	The compress_bidder_init function in archive_read_support_filter_compress.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file, which triggers an invalid left shift. **Reference: CVE-2015-8932**	https://security-tracker.debian.org/tracker/CVE-2015-8932	A- OS-CAN-UBUNT-101016/225
Overflow	2016-09-27	6.8	Multiple integer overflows in the (1) get_time_t_max and (2) get_time_t_min functions in archive_read_support_format_mtree.c in libarchive before 3.2.0 allow remote attackers to have unspecified impact via a crafted mtree file, which triggers undefined behavior. **Reference: CVE-2015-8931**	https://github.com/libarchive/libarchive/issues/539	A- OS-CAN-UBUNT-101016/226
Denial of Service	2016-09-27	4.3	The archive_read_format_tar_read_header function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tar file. **Reference: CVE-2015-8924**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/227
Denial of Service	2016-09-27	4.3	The process_extra function in libarchive before 3.2.0 uses the size field and a signed number in an offset, which allows remote attackers to cause	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-	A- OS-CAN-UBUNT-101016/228

			a denial of service (crash) via a crafted zip file. **Reference: CVE-2015-8923**	3090544.html	
Denial of Service	2016-09-27	5	The ae_strtofflags function in archive_entry.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file. **Reference: CVE-2015-8921**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/229
Denial of Service	2016-09-27	4.3	The _ar_read_header function in archive_read_support_format_ar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds stack read) via a crafted ar file. **Reference: CVE-2015-8920**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/230
Denial of Service; Overflow	2016-09-27	5	The lha_read_file_extended_header function in archive_read_support_format_lha.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap) via a crafted (1) lzh or (2) lha file. **Reference: CVE-2015-8919**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/231
Denial of Service	2016-09-30	4.3	The read_CodersInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted 7z file, related to	https://www.suse.com/security/cve/CVE-2015-8922.html	A- OS-CAN-UBUNT-101016/232

			the _7z_folder struct. **Reference: CVE-2015-8922**		
Denial of Service; Overflow	2016-09-20	4.3	Integer overflow in the archive_read_format_tar_skip function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file. **Reference: CVE-2015-8933**	https://github.com/libarchive/libarchive/issues/548	A- OS-CAN-UBUNT-101016/233
Denial of Service	2016-09-27	4.3	The copy_from_lzss_window function in archive_read_support_format_rar.c in libarchive 3.2.0 and earlier allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted rar file. **Reference: CVE-2015-8934**	https://github.com/libarchive/libarchive/issues/521	A- OS-CAN-UBUNT-101016/234
Denial of Service	2016-09-27	5	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (infinite loop) via an ISO with a directory that is a member of itself. **Reference: CVE-2015-8930**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/235
Denial of Service	2016-09-27	4.3	The process_add_entry function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file. **Reference: CVE-2015-8928**	https://github.com/libarchive/libarchive/issues/550	A- OS-CAN-UBUNT-101016/236

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	2016-09-27	4.3	The archive_read_format_rar_read_data function in archive_read_support_format_rar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted rar archive. **Reference: CVE-2015-8926**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/237
Denial of Service	2016-09-27	4.3	The readline function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read) via a crafted mtree file, related to newline parsing. **Reference: CVE-2015-8925**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-CAN-UBUNT-101016/238
Debian					
Charybdis/Debian Linux *The charybdis project is to provide a testbed for the research and development of new features in IRC server software; Debian is a Unix-like computer operating system.*					
NA	2016-09-21	6.8	The m_authenticate function in modules/m_sasl.c in Charybdis before 3.5.3 allows remote attackers to spoof certificate fingerprints and consequently log in as another user via a crafted AUTHENTICATE parameter. **Reference: CVE-2016-7143**	https://github.com/charybdis-ircd/charybdis/commit/818a3fda944b26d4814132cee14cfda4ea4aa824	A- OS-CHA-CHARY-101016/239
Debian Linux/Flex *Debian is a Unix-like computer operating system that is composed entirely of free; Flex is a tool for generating scanners.*					
Denial of Service;Execute Code	2016-09-22	7.5	Heap-based buffer overflow in the yy_get_next_buffer	https://github.com/westes/flex/commit	A- OS-DEB-DEBIA-101016/240

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

Overflow			function in Flex before 2.6.1 might allow context-dependent attackers to cause a denial of service or possibly execute arbitrary code via vectors involving num_to_read. **Reference: CVE-2016-6354**	/a5cbe929ac3255d371e698f62dc256afe7006466	
Debian Linux/Inspircd *Debian is an operating system and a distribution of Free Software; InspIRCd is a modular Internet Relay Chat (IRC) server written in C++ for Linux, BSD, Windows and Mac OS X systems*					
NA	2016-09-28	4.3	The m_sasl module in InspIRCd before 2.0.23, when used with a service that supports SASL_EXTERNAL authentication, allows remote attackers to spoof certificate fingerprints and consequently log in as another user via a crafted SASL message. **Reference: CVE-2016-7142**	https://github.com/inspircd/inspircd/commit/74fafb7f11b06747f69f182ad5e3769b665eea7a	A- OS-DEB-DEBIA-101016/241
Debian Linux/Openjpeg *Debian is a Unix-like computer operating system that is composed entirely of free; OpenJPEG is an open-source JPEG 2000 codec written in C language software, most of which is under the GNU General Public License, and packaged by a group of individuals called the Debian Project.*					
NA	2016-09-21	7.5	Use-after-free vulnerability in the opj_j2k_write_mco function in j2k.c in OpenJPEG before 2.1.1 allows remote attackers to have unspecified impact via unknown vectors. **Reference: CVE-2015-8871**	https://github.com/uclouvain/openjpeg/issues/563	A- OS-DEB-DEBIA-101016/242
Debian Linux/Wireshark *Debian systems currently use the Linux kernel or the FreeBSD kernel; Wireshark is a network protocol analyzer for Unix and Windows.*					
Denial of Service	2016-09-29	4.3	epan/dissectors/packet-ipmi-trace.c in the IPMI	https://www.wireshark.org	A- OS-DEB-DEBIA-

			trace dissector in Wireshark 2.x before 2.0.6 does not properly consider whether a string is constant, which allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted packet. **Reference: CVE-2016-7180**	/security/wnpa-sec-2016-55.html	101016/243
Denial of Service; Overflow	2016-09-29	4.3	Stack-based buffer overflow in epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000 dissector in Wireshark 2.x before 2.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted packet. **Reference: CVE-2016-7179**	https://code.wireshark.org/review/17095	A- OS-DEB-DEBIA-101016/244
Denial of Service	2016-09-29	4.3	epan/dissectors/packet-umts_fp.c in the UMTS FP dissector in Wireshark 2.x before 2.0.6 does not ensure that memory is allocated for certain data structures, which allows remote attackers to cause a denial of service (invalid write access and application crash) via a crafted packet. **Reference: CVE-2016-7178**	https://code.wireshark.org/review/17094	A- OS-DEB-DEBIA-101016/245
Denial of Service; Overflow	2016-09-29	4.3	epan/dissectors/packet-catapult-dct2000.c in the Catapult DCT2000 dissector in Wireshark 2.x before 2.0.6 does not restrict the number of channels, which allows remote attackers to cause	https://code.wireshark.org/review/17096	A- OS-DEB-DEBIA-101016/246

			a denial of service (buffer over-read and application crash) via a crafted packet. **Reference: CVE-2016-7177**		
Denial of Service; Overflow	2016-09-30	4.3	epan/dissectors/packet-h225.c in the H.225 dissector in Wireshark 2.x before 2.0.6 calls snprintf with one of its input buffers as the output buffer, which allows remote attackers to cause a denial of service (copy overlap and application crash) via a crafted packet. **Reference: CVE-2016-7176**	https://www.wireshark.org/security/wnpa-sec-2016-51.html	A- OS-DEB-DEBIA-101016/247
Execute Code Overflow	2016-09-21	6.8	Integer overflow in the opj_pi_create_decode function in pi.c in OpenJPEG allows remote attackers to execute arbitrary code via a crafted JP2 file, which triggers an out-of-bounds read or write. **Reference: CVE-2016-7163**	https://github.com/uclouvain/openjpeg/pull/809	A- OS-DEB-DEBIA-101016/248
Fedora					
Fedora/Leap/Sqlite *Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat.; LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution; SQLite is an embedded relational database engine.*					
Denial of Service; Gain Information	2016-09-28	4.6	os_unix.c in SQLite before 3.13.0 improperly implements the temporary directory search algorithm, which might allow local users to obtain sensitive information, cause a denial of service (application crash), or	https://www.sqlite.org/releaselog/3_13_0.html	A- OS-FED-FEDOR-101016/249

			have unspecified other impact by leveraging use of the current working directory for temporary files. **Reference: CVE-2016-6153**		
Fedora/Linux/Freeipa *The Linux kernel is a Unix-like computer operating system kernel. The Linux operating system is based on it and deployed on both traditional computer systems such as personal computers and servers, usually in the form of Linux distributions/ Fedora (formerly Fedora Core) is an operating system based on the Linux kernel, developed by the community-supported Fedora Project and sponsored by Red Hat.*					
NA	2016-09-28	4	The cert_revoke command in FreeIPA does not check for the "revoke certificate" permission, which allows remote authenticated users to revoke arbitrary certificates by leveraging the "retrieve certificate" permission. **Reference: CVE-2016-5404**	https://fedorahosted.org/freeipa/ticket/6232	A- OS-FED-FEDOR-101016/250
Iperf/Suse Package Hub For Suse Linux Enterprise/Leap; Opensuse *Iperf is a commonly used network testing tool that can create Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) data streams and measure the throughput of a network that is carrying them; SUSE Package Hub packages are built and maintained by a community of users and "packagers" utilizing the Open Build Service.*					
Denial of Service; Execute Code ;Overflow	2016-09-28	7.5	The parse_string function in cjson.c in the cJSON library mishandles UTF8/16 strings, which allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a non-hex character in a JSON string, which triggers a heap-based buffer overflow. **Reference: CVE-2016-4303**	http://software.es.net/iperf/news.html#security-issue-iperf-3-1-3-iperf-3-0-12-released	A- OS-IPE-IPERF-101016/251
Libarchive/ Libtiff/Microsoft/Novell					
Libarchive/Suse Linux Enterprise Desktop;Suse Linux Enterprise Server;Suse Linux					

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

Enterprise Software Development Kit *Libarchive is an open-source BSD-licensed C programming library that provides streaming access to a variety of different archive formats, including tar, cpio, pax, Zip, and ISO9660 images.*					
Denial of Service; Overflow	2016-09-20	5	The archive_string_append function in archive_string.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted cab files, related to "overlapping memcpy." **Reference: CVE-2015-8918**	https://github.com/libarchive/libarchive/issues/506	A- OS-LIB-LIBAR-101016/252
Libarchive/Linux *The libarchive library provides a flexible interface for reading and writing streaming archive files such as tar and cpio.*					
Denial of Service; Execute Code Overflow	2016-09-28	7.5	Integer overflow in the ISO9660 writer in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a buffer overflow. **Reference: CVE-2016-6250**	https://github.com/libarchive/libarchive/issues/711	A- OS-LIB-LIBAR-101016/253
Libarchive/Linux/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Hpc Node Eus;Enterprise Linux Server;Enterprise Linux Server Aus;Enterprise Linux Server Eus;Enterprise Linux Workstation *Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smart-phones and network servers; Libarchive is an open-source BSD-licensed C programming library that provides streaming access to a variety of different archive formats, including tar, cpio, pax, Zip, and ISO9660 images; Red Hat Enterprise Linux delivers military-grade security, 99.999% uptime, support for business-critical workloads; Enterprise Linux Hpc Node certified Linux operating systems designed for everything from workstations to mission-critical enterprise computing and is certified by top enterprise software vendors.*					
Denial of Service	2016-09-28	4.3	libarchive before 3.2.0 does not limit the number of recursive	http://www.oracle.com/technetwork/top	A- OS-LIB-LIBAR-101016/254

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

			decompressions, which allows remote attackers to cause a denial of service (memory consumption and application crash) via a crafted gzip file. **Reference: CVE-2016-7166**	ics/security/linuxbulletinjul2016-3090544.html	
Denial of Service; Overflow	2016-09-28	4.3	Integer overflow in the ISO parser in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a crafted ISO file. **Reference: CVE-2016-5844**	https://github.com/libarchive/libarchive/issues/717	A- OS-LIB-LIBAR-101016/255
Denial of Service	2016-09-28	5	The archive_read_format_cpio_read_header function in archive_read_support_format_cpio.c in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a CPIO archive with a large symlink. **Reference: CVE-2016-4809**	https://github.com/libarchive/libarchive/issues/705	A- OS-LIB-LIBAR-101016/256
Execute Code Overflow	2016-09-27	6.8	Heap-based buffer overflow in the parse_codes function in archive_read_support_format_rar.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a RAR file with a zero-sized dictionary. **Reference: CVE-2016-4302**	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html	A- OS-LIB-LIBAR-101016/257
Execute Code Overflow	2016-09-27	6.8	Integer overflow in the read_SubStreamsInfo function in archive_read_support_for	https://github.com/libarchive/libarchive/issues/718	A- OS-LIB-LIBAR-101016/258

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

			mat_7zip.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a 7zip file with a large number of substreams, which triggers a heap-based buffer overflow. **Reference: CVE-2016-4300**		
Denial of Service; Overflow	2016-09-20	4.3	Memory leak in the __archive_read_get_extract function in archive_read_extract2.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service via a tar file. **Reference: CVE-2015-8929**	https://github.com/libarchive/libarchive/issues/517	A- OS-LIB-LIBAR-101016/259
NA	2016-09-27	5	The sandboxing code in libarchive 3.2.0 and earlier mishandles hardlink archive entries of non-zero data size, which might allow remote attackers to write to arbitrary files via a crafted archive file. **Reference: CVE-2016-5418**	https://github.com/libarchive/libarchive/issues/746	A- OS-LIB-LIBAR-101016/260
Libtiff/Vm Server *Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files;A virtual machine server hosts or runs virtual machines that run various operating systems and act as full computing platforms on their own through emulation and virtualization.*					
Denial of Service; Execute Code Overflow	2016-09-27	6.8	Heap-based buffer overflow in the loadImage function in the tiffcrop tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image with zero tiles.	https://bugzilla.redhat.com/show_bug.cgi?id=1326249	A- OS-LIB-LIBTI-101016/261

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

			Reference: CVE-2016-3991		
Denial of Service; Execute Code Overflow	2016-09-27	6.8	Heap-based buffer overflow in the horizontalDifference8 function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image to tiffcp. **Reference: CVE-2016-3990**	https://bugzilla.redhat.com/show_bug.cgi?id=1326246	A- OS-LIB-LIBTI-101016/262
Denial of Service; Execute Code Overflow	2016-09-27	6.8	Multiple integer overflows in the (1) cvt_by_strip and (2) cvt_by_tile functions in the tiff2rgba tool in LibTIFF 4.0.6 and earlier, when -b mode is enabled, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write. **Reference: CVE-2016-3945**	https://bugzilla.redhat.com/show_bug.cgi?id=1325093	A- OS-LIB-LIBTI-101016/263
Denial of Service; Execute Code	2016-09-27	6.8	The _TIFFVGetField function in tif_dirinfo.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image. **Reference: CVE-2016-3632**	http://bugzilla.maptools.org/show_bug.cgi?id=2549	A- OS-LIB-LIBTI-101016/264

Edge/Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2012

Windows is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft. It consists of several families of operating systems.Windows Server series is Microsoft Windows server line of operating systems.

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	2016-09-26	4.3	The PDF library in Microsoft Edge, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allows remote attackers to obtain sensitive information via a crafted web site, aka "PDF Library Information Disclosure Vulnerability," a different vulnerability than CVE-2016-3370. **Reference: CVE-2016-3374**	NA	A- OS-MIC-EDGE/-101016/265
Leap/Libstorage;Libstorage-ng/Yast-storage *LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution; libstorage provides a vendor agnostic storage orchestration model, API, and reference client and server implementations;Evaluating use of boost graph library in libstorage;This is a YaST storage library, it uses libstorage backend.*					
Gain Information	2016-09-28	1.2	libstorage, libstorage-ng, and yast-storage improperly store passphrases for encrypted storage devices in a temporary file on disk, which might allow local users to obtain sensitive information by reading the file, as demonstrated by /tmp/libstorage-XXXXXX/pwdf. **Reference: CVE-2016-5746**	https://github.com/yast/yast-storage/pull/227	A- OS-NOV-LEAP/-101016/266
Leap;Opensuse/Authoritative Server *LEAP Legal Software provides a completely integrated Legal Case Management & Legal Accounting Solution;An authoritative Nameserver is a nameserver (DNS Server) that holds the actual DNS records (A, CNAME, PTR, etc) for a particular domain/ address. A recursive resolver would be a DNS server that queries an authoritative nameserver to resolve a domain/ address.*					
Denial of Service	2016-09-27	7.1	PowerDNS (aka pdns) Authoritative Server before 4.0.1 allows remote primary DNS servers to cause a denial of service	https://doc.powerdns.com/md/changelog/#powerdns-	A- OS-NOV-LEAP;-101016/267

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

			(memory exhaustion and secondary DNS server crash) via a large (1) AXFR or (2) IXFR response. **Reference: CVE-2016-6172**	authoritative-server-401	
Operating System (OS)					
Apple					
Apple Tv; Iphone Os; Mac Os X; Watch Os *Apple TV is a digital media player and a micro-console developed and sold by Apple Inc.; iPhone OS is a mobile operating system created and developed by Apple Inc.; MacOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc.*					
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	IOAcceleratorFamily in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4726**	https://support.apple.com/HT207170	O-APP-APPLE-101016/268
Denial of Service;Execute Code ;Memory Corruption	2016-09-27	9.3	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4778**	https://support.apple.com/HT207170	O-APP-APPLE-101016/269
Denial of Service; Execute Code	2016-09-27	9.3	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (invalid	https://support.apple.com/HT207170	O-APP-APPLE-101016/270

			pointer dereference) via a crafted app. **Reference: CVE-2016-4777**		
Denial of Service; Gain Information	2016-09-27	4.3	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to obtain sensitive memory-layout information or cause a denial of service (out-of-bounds read) via a crafted app, a different vulnerability than CVE-2016-4773 and CVE-2016-4774. **Reference: CVE-2016-4776**	https://support.apple.com/HT207170	O-APP-APPLE-101016/271
Execute Code	2016-09-27	9.3	Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 mishandle signed disk images, which allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference: CVE-2016-4753**	https://support.apple.com/HT207143	O-APP-APPLE-101016/272
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	libxslt in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4738**	https://support.apple.com/HT207170	O-APP-APPLE-101016/273
Denial of Service; Execute Code Overflow	2016-09-27	10	Audio in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote	https://support.apple.com/HT207170	O-APP-APPLE-101016/274

;Memory Corruption			attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2016-4702**		
Overflow Gain Information	2016-09-26	4.3	Buffer overflow in FontParser in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to obtain sensitive information from process memory via a crafted font file. **Reference: CVE-2016-4718**	https://support.apple.com/HT207170	O-APP-APPLE-101016/275
Denial of Service; Execute Code	2016-09-26	9.3	CoreCrypto in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via a crafted app. **Reference: CVE-2016-4712**	https://support.apple.com/HT207170	O-APP-APPLE-101016/276
Gain Information	2016-09-26	4.3	CFNetwork in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 misparses the Set-Cookie header, which allows remote attackers to obtain sensitive information via a crafted HTTP response. **Reference: CVE-2016-4708**	https://support.apple.com/HT207170	O-APP-APPLE-101016/277
Denial of Service; Execute Code Overflow ;Memory	2016-09-26	10	libxml2 in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to	https://support.apple.com/HT207170	O-APP-APPLE-101016/278

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

Corruption			execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document. **Reference: CVE-2016-4658**		
Denial of Service; Gain Information	2016-09-27	5.8	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to obtain sensitive memory-layout information or cause a denial of service (out-of-bounds read) via a crafted app, a different vulnerability than CVE-2016-4773 and CVE-2016-4776. **Reference: CVE-2016-4774**	https://support.apple.com/HT207170	O-APP-APPLE-101016/279
Denial of Service; Gain Information	2016-09-27	5.8	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows attackers to obtain sensitive memory-layout information or cause a denial of service (out-of-bounds read) via a crafted app, a different vulnerability than CVE-2016-4774 and CVE-2016-4776. **Reference: CVE-2016-4773**	https://support.apple.com/HT207170	O-APP-APPLE-101016/280
Denial of Service	2016-09-27	5	The kernel in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to cause a denial of service (unintended lock) via unspecified vectors. **Reference: CVE-2016-**	https://support.apple.com/HT207170	O-APP-APPLE-101016/281

			4772		
Denial of Service; Overflow ;Memory Corruption Gain Information	2016-09-27	5.8	IOAcceleratorFamily in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (memory corruption) via a crafted web site. **Reference: CVE-2016-4725**	https://support.apple.com/HT207170	O-APP-APPLE-101016/282
Denial of Service; Overflow ;Gain Privileges ;Memory Corruption	2016-09-27	7.2	The kernel in Apple OS X before 10.12, tvOS before 10, and watchOS before 3 allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors. **Reference: CVE-2016-4775**	https://support.apple.com/HT207170	O-APP-APPLE-101016/283
Iphone Os *iPhone OS is a mobile operating system created and developed by Apple Inc.*					
Gain Information	2016-09-26	2.1	Printing UIKit in Apple iOS before 10 mishandles environment variables, which allows local users to discover cleartext AirPrint preview content by reading a temporary file. **Reference: CVE-2016-4749**	https://support.apple.com/HT207143	O-APP-IPHON-101016/284
Gain Information	2016-09-26	4.3	Mail in Apple iOS before 10 mishandles certificates, which makes it easier for man-in-the-middle attackers to discover mail credentials via unspecified vectors. **Reference: CVE-2016-4747**	https://support.apple.com/HT207143	O-APP-IPHON-101016/285

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	2016-09-26	5	The Keyboards component in Apple iOS before 10 does not properly use a cache for auto-correct suggestions, which allows remote attackers to obtain sensitive information in opportunistic circumstances by leveraging an unintended correction. **Reference: CVE-2016-4746**	https://support.apple.com/HT207143	O-APP-IPHON-101016/286
NA	2016-09-26	4.3	The Assets component in Apple iOS before 10 allows man-in-the-middle attackers to block software updates via vectors related to lack of an HTTPS session for retrieving updates. **Reference: CVE-2016-4741**	https://support.apple.com/HT207143	O-APP-IPHON-101016/287
Gain Information	2016-09-26	1.9	Apple iOS before 10, when Handoff for Messages is used, does not ensure that a Messages signin has occurred before displaying messages, which might allow attackers to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4740**	https://support.apple.com/HT207143	O-APP-IPHON-101016/288
Gain Information	2016-09-26	4.3	The Sandbox Profiles component in Apple iOS before 10 does not properly restrict access to directory metadata for SMS draft directories, which allows attackers to discover text-message recipients via a crafted app. **Reference: CVE-2016-**	https://support.apple.com/HT207143	O-APP-IPHON-101016/289

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

			4620		
Iphone Os; Mac Os X *iPhone OS is a mobile operating system created and developed by Apple Inc.;MacOS is the current series of Unix-based graphical operating systems developed and marketed byApple Inc.*					
Denial of Service; Execute Code	2016-09-26	9.3	IOAcceleratorFamily in Apple iOS before 10 and OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference: CVE-2016-4724**	https://support.apple.com/HT207170	O-APP-IPHON-101016/290
Gain Information	2016-09-26	4.3	The IDS - Connectivity component in Apple iOS before 10 and OS X before 10.12 allows man-in-the-middle attackers to conduct Call Relay spoofing attacks and obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4722**	https://support.apple.com/HT207170	O-APP-IPHON-101016/291
NA	2016-09-26	5	CCrypt in corecrypto in CommonCrypto in Apple iOS before 10 and OS X before 10.12 allows attackers to discover cleartext information by leveraging a function call that specifies the same buffer for input and output. **Reference: CVE-2016-4711**	https://support.apple.com/HT207170	O-APP-IPHON-101016/292
NA	2016-09-26	2.1	CFNetwork in Apple iOS before 10 and OS X before 10.12 mishandles Local Storage deletion, which allows local users to	https://support.apple.com/HT207170	O-APP-IPHON-101016/293

			discover the visited web sites of arbitrary users via unspecified vectors. **Reference: CVE-2016-4707**		
Bypass Gain Information	2016-09-27	4.3	The kernel in Apple iOS before 10 and OS X before 10.12 allows local users to bypass intended file-access restrictions via a crafted directory pathname. **Reference: CVE-2016-4771**	https://support.apple.com/HT207170	O-APP-IPHON-101016/294
Denial of Service; Execute Code Overflow ;Memory Corruption	2016-09-27	9.3	S2 Camera in Apple iOS before 10 and OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4750**	https://support.apple.com/HT207170	O-APP-IPHON-101016/295
Execute Code	2016-09-27	9.3	AppleMobileFileIntegrity in Apple iOS before 10 and OS X before 10.12 mishandles process entitlement and Team ID values in the task port inheritance policy, which allows attackers to execute arbitrary code in a privileged context via a crafted app. **Reference: CVE-2016-4698**	https://support.apple.com/HT207170	O-APP-IPHON-101016/296
Iphone Os; Watchos *iPhone OS is a mobile operating system created and developed by Apple Inc.*					
Gain Information	2016-09-26	4.3	The GeoServices component in Apple iOS before 10 and watchOS before 3 does not properly restrict access to PlaceData information, which	https://support.apple.com/HT207141	O-APP-IPHON-101016/297

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

			allows attackers to discover physical locations via a crafted application. **Reference: CVE-2016-4719**		
Mac Os X *MacOS is the current series of Unix-based graphical operating systems developed and marketed byApple Inc.*					
Bypass	2016-09-26	4.6	Perl in Apple OS X before 10.12 allows local users to bypass the taint-mode protection mechanism via a crafted environment variable. **Reference: CVE-2016-4748**	https://support.apple.com/HT207170	O-APP-MACO-101016/298
Gain Information	2016-09-26	4.3	NSSecureTextField in Apple OS X before 10.12 does not enable Secure Input, which allows attackers to discover credentials via a crafted app. **Reference: CVE-2016-4742**	https://support.apple.com/HT207170	O-APP-MACO-101016/299
Gain Information	2016-09-26	4.3	mDNSResponder in Apple OS X before 10.12, when VMnet.framework is used, arranges for a DNS proxy to listen on all interfaces, which allows remote attackers to obtain sensitive information by sending a DNS query to an unintended interface. **Reference: CVE-2016-4739**	https://support.apple.com/HT207170	O-APP-MACO-101016/300
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	IOThunderboltFamily in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4727**	https://support.apple.com/HT207170	O-APP-MACO-101016/301
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	Intel Graphics Driver in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption)	https://support.apple.com/HT207170	O-APP-MACO-101016/302

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

			via a crafted app. **Reference: CVE-2016-4723**		
Denial of Service	2016-09-26	5	The File Bookmark component in Apple OS X before 10.12 mishandles scoped-bookmark file descriptors, which allows attackers to cause a denial of service via a crafted app. **Reference: CVE-2016-4717**	https://support.apple.com/HT207170	O-APP-MAC O-101016/303
Gain Privileges	2016-09-26	7.2	diskutil in DiskArbitration in Apple OS X before 10.12 allows local users to gain privileges via unspecified vectors. **Reference: CVE-2016-4716**	https://support.apple.com/HT207170	O-APP-MAC O-101016/304
NA	2016-09-26	4.3	CoreDisplay in Apple OS X before 10.12 allows attackers to view arbitrary users' screens by leveraging screen-sharing access. **Reference: CVE-2016-4713**	https://support.apple.com/HT207170	O-APP-MAC O-101016/305
NA	2016-09-26	7.2	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4709. **Reference: CVE-2016-4710**	https://support.apple.com/HT207170	O-APP-MAC O-101016/306
NA	2016-09-26	7.2	WindowServer in Apple OS X before 10.12 allows local users to obtain root access via vectors that leverage "type confusion," a different vulnerability than CVE-2016-4710. **Reference: CVE-2016-4709**	https://support.apple.com/HT207170	O-APP-MAC O-101016/307
Denial of Service	2016-09-26	4.9	cd9660 in Apple OS X before 10.12 allows local users to cause a denial of service via unspecified vectors. **Reference: CVE-2016-4706**	https://support.apple.com/HT207170	O-APP-MAC O-101016/308
Denial of	2016-09-26	9.3	Bluetooth in Apple OS X	https://sup	O-APP-MAC

Service;Execute Code Overflow ;Memory Corruption			before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4703**	port.apple.com/HT207170	O-101016/309
Denial of Service	2016-09-26	2.1	Application Firewall in Apple OS X before 10.12 allows local users to cause a denial of service via vectors involving a crafted SO_EXECPATH environment variable. **Reference: CVE-2016-4701**	https://support.apple.com/HT207170	O-APP-MAC O-101016/310
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4699. **Reference: CVE-2016-4700**	https://support.apple.com/HT207170	O-APP-MAC O-101016/311
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	AppleUUC in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app, a different vulnerability than CVE-2016-4700. **Reference: CVE-2016-4699**	https://support.apple.com/HT207170	O-APP-MAC O-101016/312
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-26	9.3	Apple HSSPI Support in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **Reference: CVE-2016-4697**	https://support.apple.com/HT207170	O-APP-MAC O-101016/313
Denial of Service;Execute Code	2016-09-26	9.3	AppleEFIRuntime in Apple OS X before 10.12 allows attackers to execute arbitrary code in a privileged	https://support.apple.com/HT207170	O-APP-MAC O-101016/314

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

			context or cause a denial of service (NULL pointer dereference) via a crafted app. **Reference: CVE-2016-4696**		
Denial of Service;Execute Code Overflow ;Memory Corruption	2016-09-27	6.8	Apple Type Services (ATS) in Apple OS X before 10.12 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font file. **Reference: CVE-2016-4779**	https://support.apple.com/HT207170	O-APP-MAC O-101016/315
Gain Information	2016-09-27	2.1	Terminal in Apple OS X before 10.12 uses weak permissions for the .bash_history and .bash_session files, which allows local users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-4755**	https://support.apple.com/HT207170	O-APP-MAC O-101016/316
Gain Information	2016-09-27	4.3	The SecKeyDeriveFromPassword function in Apple OS X before 10.12 does not use the CF_RETURNS_RETAINED keyword, which allows attackers to obtain sensitive information from process memory by triggering key derivation. **Reference: CVE-2016-4752**	https://support.apple.com/HT207170	O-APP-MAC O-101016/317
Gain Information	2016-09-27	5	The Kerberos 5 (aka krb5) PAM module in Apple OS X before 10.12 does not use constant-time operations for determining username validity, which makes it easier for remote attackers to enumerate user accounts via a timing side-channel attack. **Reference: CVE-2016-4745**	https://support.apple.com/HT207170	O-APP-MAC O-101016/318

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 ;Memory Corruption	2016-09-27	9.3	libarchive in Apple OS X before 10.12 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted file. **Reference: CVE-2016-4736**	https://support.apple.com/HT207170	O-APP-MACO-101016/319
Gain Information	2016-09-27	4.3	The Date & Time Pref Pane component in Apple OS X before 10.12 mishandles the .GlobalPreferences file, which allows attackers to discover a user's location via a crafted app. **Reference: CVE-2016-4715**	https://support.apple.com/HT207170	O-APP-MACO-101016/320
Mac Os X;Os X Server *MacOS is the current series of Unix-based graphical operating systems developed and marketed by Apple Inc; OS X Server is a separately sold operating system add-on which provides additional server programs and management and administration tools for macOS.*					
	2016-09-26	7.5	The Apache HTTP Server in Apple OS X before 10.12 and OS X Server before 5.2 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted CGI client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue, a related issue to CVE-2016-5387. **Reference: CVE-2016-4694**	https://support.apple.com/HT207171	O-APP-MACO-101016/321
Os X Server *OS X Server is a separately sold operating system add-on which provides additional server programs and management and administration tools for macOS.*					
NA	2016-09-27	5	ServerDocs Server in Apple OS X Server before 5.2	https://support.apple.c	O-APP-OS X -101016/322

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

			supports the RC4 cipher, which might allow remote attackers to defeat cryptographic protection mechanisms via unspecified vectors. **Reference: CVE-2016-4754**	om/HT207171	
Aver					
Eh6108h+ Firmware: *NA*					
Gain Information	2016-09-19	5	AVer Information EH6108H+ devices with firmware X9.03.24.00.07l store passwords in a cleartext base64 format and require cleartext credentials in HTTP Cookie headers, which allows context-dependent attacks to obtain sensitive information by reading these strings. **Reference: CVE-2016-6537**	http://www.kb.cert.org/vuls/id/667480	O-AVE-EH610-101016/323
Bypass	2016-09-19	10	The /setup URI on AVer Information EH6108H+ devices with firmware X9.03.24.00.07l allows remote attackers to bypass intended page-access restrictions or modify passwords by leveraging knowledge of a handle parameter value. **Reference: CVE-2016-6536**	http://www.kb.cert.org/vuls/id/667480	O-AVE-EH610-101016/324
Gain Information	2016-09-19	10	Aver Information EH6108H+ devices with firmware X9.03.24.00.07l have hardcoded accounts, which allows remote attackers to obtain root access by leveraging knowledge of the credentials and establishing a TELNET session. **Reference: CVE-2016-6535**	http://www.kb.cert.org/vuls/id/667480	O-AVE-EH610-101016/325
Cisco					
IOS *Cisco IOS is a family of software used on most Cisco Systems routers and current Cisco network*					

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

switches.					
Cross-site scripting	2016-09-19	4.3	Cross-site scripting (XSS) vulnerability in the web framework in Cisco IOx Local Manager in IOS 15.5(2)T and IOS XE allows remote attackers to inject arbitrary web script or HTML via a crafted URL, aka Bug ID CSCuy19854. **Reference: CVE-2016-6404**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ios	O-CIS-IOS-101016/326
Denial of Service	2016-09-19	4.3	The Data in Motion (DMo) application in Cisco IOS 15.6(1)T and IOS XE, when the IOx feature set is enabled, allows remote attackers to cause a denial of service via a crafted packet, aka Bug IDs CSCuy82904, CSCuy82909, and CSCuy82912. **Reference: CVE-2016-6403**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160914-ios-xe	O-CIS-IOS-101016/327
Execute Code	2016-09-23	7.2	iox in Cisco IOS, possibly 15.6 and earlier, and IOS XE, possibly 3.18 and earlier, allows local users to execute arbitrary IOx Linux commands on the guest OS via crafted iox command-line options, aka Bug ID CSCuz59223. **Reference: CVE-2016-6414**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-iox	O-CIS-IOS-101016/328
NA	2016-09-26	4.3	The Cisco Application-hosting Framework (CAF) component in Cisco IOS 15.6(1)T1 and IOS XE, when the IOx feature set is enabled, allows man-in-the-middle attackers to trigger arbitrary downloads via crafted HTTP headers, aka Bug ID CSCuz84773. **Reference: CVE-2016-6412**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-caf1	O-CIS-IOS-101016/329
NA	2016-09-27	6.8	The Cisco Application-hosting Framework (CAF)	http://tools.cisco.com	O-CIS-IOS-101016/330

			component in Cisco IOS 15.6(1)T1 and IOS XE, when the IOx feature set is enabled, allows remote authenticated users to read arbitrary files via unspecified vectors, aka Bug ID CSCuy19856. **Reference: CVE-2016-6410**	/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-caf	
Denial of Service	2016-09-27	4.3	The Data in Motion (DMo) component in Cisco IOS 15.6(1)T and IOS XE, when the IOx feature set is enabled, allows remote attackers to cause a denial of service (out-of-bounds access) via crafted traffic, aka Bug ID CSCuy54015. **Reference: CVE-2016-6409**	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160921-dmo	O-CIS-IOS-101016/331
Gain Information	2016-09-30	5	The server IKEv1 implementation in Cisco IOS 12.2 through 12.4 and 15.0 through 15.6, IOS XE through 3.18S, IOS XR 4.3.x and 5.0.x through 5.2.x, and PIX before 7.0 allows remote attackers to obtain sensitive information from device memory via a Security Association (SA) negotiation request, aka Bug IDs CSCvb29204 and CSCvb36055 or BENIGNCERTAIN. **Reference: CVE-2016-6415**	NA	O-CIS-IOS-101016/332
Ios Xr *IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end Network Converging System(NCS), carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.*					
Denial of Service	2016-09-19	5	Cisco IOS XR 6.0 and 6.0.1 on NCS 6000 devices allows remote attackers to cause a denial of service (OSPFv3 process reload) via crafted OSPFv3 packets, aka Bug ID CSCuz66289.	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	O-CIS-IOS X-101016/333

			Reference: CVE-2016-1433	sa-20160914-iosxr	
IOS; Ios Xe *Cisco IOS is a family of software used on most Cisco Systems routers and current Cisco network switches; IOS XE represents the continuing evolution of Cisco's pre-eminent IOS operating system.*					
Bypass	2016-09-23	4.3	The Zone-Based Firewall (ZBFW) functionality in Cisco IOS, possibly 15.4 and earlier, and IOS XE, possibly 3.13 and earlier, mishandles zone checking for existing sessions, which allows remote attackers to bypass intended resource-access restrictions via spoofed traffic that matches one of these sessions, aka Bug IDs CSCun94946 and CSCun96847. **Reference: CVE-2014-2146**	NA	O-CIS-IOSI-101016/334
Citrix					
Linux Virtual Delivery Agent *The Virtual Delivery Agent (VDA) enables connections to applications and desktops. The VDA is installed on the machine that runs the applications or virtual desktops for the user. It enables the machines to register with Delivery Controllers and manage the High Definition eXperience (HDX) connection to a user device.*					
Gain Privileges	2016-09-27	7.2	Citrix Linux Virtual Delivery Agent (aka VDA, formerly Linux Virtual Desktop) before 1.4.0 allows local users to gain root privileges via unspecified vectors. **Reference: CVE-2016-6276**	http://support.citrix.com/article/CTX216628	O-CIT-LINUX-101016/335
Google					
Chrome OS *Chrome OS is an operating system designed by Google that is based on the Linux kernel and uses the Google Chrome web browser as its principal user interface. As a result, Chrome OS primarily supports web applications.*					
Denial of Service	2016-09-27	6.8	Format string vulnerability in Google Chrome OS before 53.0.2785.103 allows remote attackers to cause a denial of service or possibly have	https://bugs.chromium.org/p/chromium/issues/detail?i	O-GOO-CHROM-101016/336

			unspecified other impact via unknown vectors. **Reference: CVE-2016-5169**	d=635879	
Huawei					
Ac6003 Firmware;Ac6005 Firmware;Ac6605 Firmware;Acu2 Firmware: *NA*					
Denial of Service	2016-09-22	6.8	Huawei AC6003, AC6005, AC6605, and ACU2 access controllers with software before V200R006C10SPC200 allows remote authenticated users to cause a denial of service (device restart) via crafted CAPWAP packets. **Reference: CVE-2016-6824**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160817-01-ac-en	O-HUA-AC600-101016/337
Ar Firmware; Netengine 16ex Firmware *The AR Firmware Upgrade Utility is used to upgrade the firmware for many AR products. The utility itself does not include any firmware files; NetEngine Series Routers are high performance routers to power innovative enterprise applications from small to super huge scale.*					
Denial of Service	2016-09-28	6.8	Format string vulnerability in Huawei AR100, AR120, AR150, AR200, AR500, AR550, AR1200, AR2200, AR2500, AR3200, and AR3600 routers with software before V200R007C00SPC900 and NetEngine 16EX routers with software before V200R007C00SPC900 allows remote authenticated users to cause a denial of service via format string specifiers in vectors involving partial commands. **Reference: CVE-2016-6901**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160824-01-vrp-en	O-HUA-AR FI-101016/338
Honor6 Firmware; Mate S Firmware; P8 Firmware *Huawei firmware is a type of software that provides control, monitoring and data manipulation of engineered products and systems.*					
Denial of Service	2016-09-28	7.1	The video driver in Huawei Mate S smartphones with software CRR-TL00 before CRR-TL00C01B362, CRR-UL20 before CRR-UL20C00B362, CRR-CL00	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-HONOR-101016/339

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

			before CRR-CL00C92B362, and CRR-CL20 before CRR-CL20C92B362; P8 smartphones with software GRA-TL00 before GRA-TL00C01B366, GRA-UL00 before GRA-UL00C00B366, GRA-UL10 before GRA-UL10C00B366, and GRA-CL00 before GRA-CL00C92B366; and Honor 6 and Honor 6 Plus smartphones with software before 6.9.16 allows attackers to cause a denial of service (device reboot) via a crafted application. **Reference: CVE-2016-8279**	20160921-01-smartphone-en	
S12700 Firmware; S5300 Firmware; S5700 Firmware; S6300 Firmware; S6700 Firmware; S7700 Firmware; S9300 Firmware; S9700 Firmware *High-performance, super-reliable 10 GE switches with comprehensive Quality of Service and security capabilities, ideal for use as access switches in large-scale data centers and core switches in campus networks.*					
Denial of Service	2016-09-28	5	Memory leak in Huawei S9300, S5300, S5700, S6700, S7700, S9700, and S12700 devices allows remote attackers to cause a denial of service (memory consumption and restart) via a large number of malformed packets. **Reference: CVE-2016-6518**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160914-01-sep-en	O-HUA-S1270-101016/340
Usg2100 Firmware; Usg2200 Firmware; Usg5100 Firmware;Usg5500 Firmware *The USG5100 series of Huawei integrates security functions including IPS, AV, AS, URL filtering, application control, and content filtering, and other functions, such as routing, switching, high availability, VPN, NAT, bandwidth management, identity authentication, load balancing, IPv6, and visualized management to protect networks against Denial of Service attacks, worms, Trojan horses, viruses, intrusions; The USG5500 series gateways are Huawei's new 10-Gigabit unified security gateways, developed to meet the needs of carriers, large- and medium-sized enterprises and next-generation data centers.*					
Execute Code Overflow	2016-09-22	7.1	Buffer overflow in the Authentication, Authorization and Accounting (AAA) module in	http://www.huawei.com/en/psirt/security-	O-HUA-USG21-101016/341

			Huawei USG2100, USG2200, USG5100, and USG5500 unified security gateways with software before V300R001C10SPC600 allows remote authenticated RADIUS servers to execute arbitrary code by sending a crafted EAP packet. **Reference: CVE-2016-6669**	advisories/huawei-sa-20160810-01-usg-en	
Ws331a Router Firmware *Huawei WS331a mini portable wireless router.*					
Bypass	2016-09-22	6.8	The management interface of Huawei WS331a routers with software before WS331a-10 V100R001C01B112 allows remote attackers to bypass authentication and obtain administrative access by sending "special packages" to the LAN interface. **Reference: CVE-2016-6159**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160907-01-ws331a-en	O-HUA-WS331-101016/342
Cross Site Request Forgery	2016-09-22	7.1	Multiple cross-site request forgery (CSRF) vulnerabilities in Huawei WS331a routers with software before WS331a-10 V100R001C01B112 allow remote attackers to hijack the authentication of administrators for requests that (1) restore factory settings or (2) reboot the device via unspecified vectors. **Reference: CVE-2016-6158**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160907-01-ws331a-en	O-HUA-WS331-101016/343
IBM					
AIX *The AIX operating system is designed to deliver outstanding scalability, reliability, and manageability.*					
Directory Traversal	2016-09-28	4	Directory traversal vulnerability in Eclipse Help in IBM Tivoli Lightweight Infrastructure (aka LWI), as	http://aix.software.ibm.com/aix/efixes/secu	O-IBM-AIX-101016/344

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

			used in AIX 5.3, 6.1, and 7.1, allows remote authenticated users to read arbitrary files via a crafted URL. **Reference: CVE-2016-6038**	rity/pconsole_mitigation.asc	
Iodata					
Hvl-a2.0 Firmware; Hvl-a3.0 Firmware; Hvl-a4.0 Firmware; Hvl-at1.0s Firmware; Hvl-at2.0 Firmware; Hvl-at2.0a Firmware; Hvl-at3.0 Firmware; Hvl-at3.0a Firmware; Hvl-at4.0 Firmware; Hvl-at4.0a Firmware NA					
Cross Site Request Forgery	2016-09-28	6.8	Cross-site request forgery (CSRF) vulnerability on I-O DATA DEVICE HVL-A2.0, HVL-A3.0, HVL-A4.0, HVL-AT1.0S, HVL-AT2.0, HVL-AT3.0, HVL-AT4.0, HVL-AT2.0A, HVL-AT3.0A, and HVL-AT4.0A devices with firmware before 2.04 allows remote attackers to hijack the authentication of arbitrary users for requests that delete content. **Reference: CVE-2016-4845**	http://www.iodata.jp/support/information/2016/hvl-a_csrf/	O-IOD-HVL-A-101016/345
Lenovo					
Bios: *NA*					
Bypass	2016-09-23	7.2	The BIOS for Lenovo ThinkCentre E93, M6500t/s, M6600, M6600q, M6600t/s, M73p, M800, M83, M8500t/s, M8600t/s, M900, M93, and M93P devices; ThinkServer RQ940, RS140, TS140, TS240, TS440, and TS540 devices; and ThinkStation E32, P300, and P310 devices might allow local users or physically proximate attackers to bypass the Secure Boot protection mechanism by leveraging an AMI test key. **Reference: CVE-2016-5247**	https://support.lenovo.com/product_security/PS500067	O-LEN-BIOS-101016/346
Moxa					

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

Active Opc Server *Active OPC Server Lite is a software package provided by Moxa that operates as an OPC driver for an HMI or SCADA system.*					
Gain Privileges	2016-09-27	7.2	Unquoted Windows search path vulnerability in Moxa Active OPC Server before 2.4.19 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory. **Reference: CVE-2016-5793**	https://ics-cert.us-cert.gov/advisories/ICSA-16-264-01	O-MOX-ACTIV-101016/347
Siemens					
Scalance M-800 Firmware;Scalance S615 Firmware: *NA*					
Gain Information	2016-09-29	4.3	The integrated web server on Siemens SCALANCE M-800 and S615 modules with firmware before 4.02 does not set the secure flag for the session cookie in an https session, which makes it easier for remote attackers to capture this cookie by intercepting its transmission within an http session. **Reference: CVE-2016-7090**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-342135.pdf	O-SIE-SCALA-101016/348
XEN					
XEN *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.*					
Gain Privileges	2016-09-21	7.2	Xen 4.5.3, 4.6.3, and 4.7.x allow local HVM guest OS administrators to overwrite hypervisor memory and consequently gain host OS privileges by leveraging mishandling of instruction pointer truncation during emulation. **Reference: CVE-2016-7093**	http://xenbits.xen.org/xsa/xsa186-0001-x86-emulate-Correct-boundary-interactions-of-emulate.patch	O-XEN-XEN-101016/349
Denial of Service; Execute Code ;Gain Information	2016-09-22	7.2	Use-after-free vulnerability in the FIFO event channel code in Xen 4.4.x allows local guest OS	http://xenbits.xen.org/xsa/xsa188.patch	O-XEN-XEN-101016/350

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

			administrators to cause a denial of service (host crash) and possibly execute arbitrary code or obtain sensitive information via an invalid guest frame number. **Reference: CVE-2016-7154**		
Denial of Service; Overflow	2016-09-22	1.5	Buffer overflow in Xen 4.7.x and earlier allows local x86 HVM guest OS administrators on guests running with shadow paging to cause a denial of service via a pagetable update. **Reference: CVE-2016-7094**	http://xenbits.xen.org/xsa/advisory-187.html	O-XEN-XEN-101016/351
Gain Privileges	2016-09-22	6.8	The get_page_from_l3e function in arch/x86/mm.c in Xen allows local 32-bit PV guest OS administrators to gain host OS privileges via vectors related to L3 recursive pagetables. **Reference: CVE-2016-7092**	http://xenbits.xen.org/xsa/advisory-185.html	O-XEN-XEN-101016/352

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