Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Apache					
Hadoop The Apache Hadoop software library is a framework that allows for the distributed processing of large data sets across clusters of computers using simple programming models.					
NA	29/11/2016	6.5	In Apache Hadoop 2.6.x before 2.6.5 and 2.7.x before 2.7.3, a remote user who can authenticate with the HDFS NameNode can possibly run arbitrary commands with the same privileges as the HDFS service. **Reference: CVE-2016-5393**	http://mail-archives.apache.org/mod_mbox/hadoop-general/201611.mbox/%3CCAA0W1bTbUmUUSF1rjRpX-2DvWutcrPt7TJSWUcSLg1F0gyHG1Q%40mail.gmail.com%3E	A-APA-HADOO--71216/01
BOA					
BOA Boa is a discontinued since 2005 open-source small-footprint web server that is suitable for embedded applications.					
Overflow	30/11/2016	5	Buffer overflow in send_redirect() in Boa Webserver 0.92r allows remote attackers to DoS via an HTTP GET request requesting a long URI with only '/' and '.' characters. **Reference: CVE-2016-9564**	NA	A-BOA-BOA--71216/02
Cisco					
Adaptive Security Appliance Software Cisco ASA Software delivers enterprise-class security capabilities for the ASA security family in a variety of form factors.					
NA	18/11/2016	4.3	Vulnerability in the HTTP web-based management interface	https://tools.cisco.com/	A-CIS-ADAPT--

			of the Cisco Adaptive Security Appliance (ASA) could allow an unauthenticated, remote attacker to inject arbitrary XML commands on the affected system. More Information: CSCva38556. Known Affected Releases: 9.1(6.10). Known Fixed Releases: 100.11(0.75) 100.15(0.137) 100.8(40.129) 96.2(0.95) 97.1(0.55) 97.1(12.7) 97.1(6.30). **Reference: CVE-2016-6461**	security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-asa	71216/03
Application Policy Infrastructure Controller; Nx-os The Cisco Application Policy Infrastructure Controller (APIC) is the single point of policy and management of a Cisco Application Centric Infrastructure (ACI) fabric; NX-OS is a network operating system for the Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches made by Cisco Systems.					
Denial of Service; Overflow	18/11/2016	6.1	Vulnerability in the Cisco Nexus 9000 Series Platform Leaf Switches for Application Centric Infrastructure (ACI) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the affected device. This vulnerability affects Cisco Nexus 9000 Series Leaf Switches (TOR) - ACI Mode and Cisco Application Policy Infrastructure Controller (APIC). More Information: CSCuy93241. Known Affected Releases: 11.2(2x) 11.2(3x) 11.3(1x) 11.3(2x) 12.0(1x). Known Fixed Releases: 11.2(2i) 11.2(2j) 11.2(3f) 11.2(3g) 11.2(3h) 11.2(3l) 11.3(0.236) 11.3(1j) 11.3(2i) 11.3(2j) 12.0(1r). **Reference: CVE-2016-6457**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-n9kapic	A-CIS-APPLI--71216/04
Asr 5000 Series Software; Virtualized Packet Core The Cisco ASR 5000 Series was developed to address the anticipated increase in performance requirements that the next generation of the mobile Internet will bring; As the industry's most					

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

complete, fully virtualized evolved packet core, the new Cisco Ultra Packet Core (UPC) solution redefines the paradigm of agility for service providers.					
Denial of Service	18/11/2016	5	A vulnerability in the IPsec component of StarOS for Cisco ASR 5000 Series routers could allow an unauthenticated, remote attacker to terminate all active IPsec VPN tunnels and prevent new tunnels from establishing, resulting in a denial of service (DoS) condition. This vulnerability affects the following Cisco products: Cisco ASR 5000/5500 Series routers, Cisco Virtualized Packet Core (VPC). More Information: CSCva13631. Known Affected Releases: 20.0.0 20.1.0 20.2.0 20.2.3 20.2.v1 21.0.0 21.0.M0.64246. Known Fixed Releases: 20.2.3 20.2.3.65026 20.2.a4.65307 20.2.v1 20.2.v1.65353 20.3.M0.65037 20.3.T0.65043 21.0.0 21.0.0.65256 21.0.M0.64595 21.0.M0.64860 21.0.M0.65140 21.0.V0.65052 21.0.V0.65150 21.0.V0.65366 21.0.VC0.64639 21.1.A0.64861 21.1.A0.65145 21.1.PP0.65270 21.1.R0.65130 21.1.R0.65135 21.1.R0.65154 21.1.VC0.64898 21.1.VC0.65203 21.2.A0.65147. **Reference: CVE-2016-6466**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-asr	A-CIS-ASR 5--71216/05
Firesight System Software NA					
Bypass	18/11/2016	5	A vulnerability in the FTP Representational State Transfer Application Programming Interface (REST API) for Cisco Firepower System Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	A-CIS-FIRES--71216/06

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

			attacker to bypass FTP malware detection rules and download malware over an FTP connection. Cisco Firepower System Software is affected when the device has a file policy with malware block configured for FTP connections. More Information: CSCuv36188 CSCuy91156. Known Affected Releases: 5.4.0.2 5.4.1.1 5.4.1.6 6.0.0 6.1.0 6.2.0. Known Fixed Releases: 6.0.0. **Reference: CVE-2016-6460**	20161116-fss	
Telepresence Tc Software NA					
Execute Code	18/11/2016	4.9	Cisco TelePresence endpoints running either CE or TC software contain a vulnerability that could allow an authenticated, local attacker to execute a local shell command injection. More Information: CSCvb25010. Known Affected Releases: 8.1.x. Known Fixed Releases: 6.3.4 7.3.7 8.2.2 8.3.0. **Reference: CVE-2016-6459**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tp	A-CIS-TELEP--71216/07
Unified Communications Manager Cisco Unified Communications (UC) is an IP-based communications system integrating voice, video, data, and mobility products and applications. It enables more effective, secure communications and can transform the way in which we communicate.					
Cross Site Scripting	18/11/2016	4.3	A vulnerability in several parameters of the ccmivr page of Cisco Unified Communication Manager (CallManager) could allow an unauthenticated, remote attacker to launch a cross-site scripting (XSS) attack against a user of the web interface on the affected system. More Information: CSCvb37121. Known Affected Releases: 11.5(1.2). Known	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-ucm	A-CIS-UNIFI--71216/08

			Fixed Releases: 11.5(1.11950.96) 11.5(1.12900.2) 12.0(0.98000.133) 12.0(0.98000.313) 12.0(0.98000.404). **Reference: CVE-2016-6472**		
Dbd-mysql Project					
Dbd-mysql DBD-mysql is the MySQL driver for the Perl5 Database Interface (DBI).					
NA	29/11/2016	6.8	There is a vulnerability of type use-after-free affecting DBD::mysql (aka DBD-mysql or the Database Interface (DBI) MySQL driver for Perl) 3.x and 4.x before 4.041 when used with mysql_server_prepare=1. **Reference: CVE-2016-1251**	http://www.openwall.com/lists/oss-security/2016/11/28/2	A-DBD-DBD-M--71216/09
Drupal					
Drupal Drupal is a scalable, open platform for web content management and digital experiences.					
Denial of Service	25/11/2016	4.3	The transliterate mechanism in Drupal 8.x before 8.2.3 allows remote attackers to cause a denial of service via a crafted URL. **Reference: CVE-2016-9452**	https://www.drupal.org/SA-CORE-2016-005	A-DRU-DRUPA--71216/10
NA	25/11/2016	4.9	Confirmation forms in Drupal 7.x before 7.52 make it easier for remote authenticated users to conduct open redirect attacks via unspecified vectors. **Reference: CVE-2016-9451**	https://www.drupal.org/SA-CORE-2016-005	A-DRU-DRUPA--71216/11
NA	25/11/2016	5	The user password reset form in Drupal 8.x before 8.2.3 allows remote attackers to conduct cache poisoning attacks by leveraging failure to specify a correct cache context. **Reference: CVE-2016-9450**	https://www.drupal.org/SA-CORE-2016-005	A-DRU-DRUPA--71216/12
Gain Information	25/11/2016	4	The taxonomy module in Drupal 7.x before 7.52 and 8.x before 8.2.3 might allow remote authenticated users to obtain sensitive information about	https://www.drupal.org/SA-CORE-2016-005	A-DRU-DRUPA--71216/13

			taxonomy terms by leveraging inconsistent naming of access query tags. **Reference: CVE-2016-9449**		
Exponentcms					
Exponent Cms Exponent CMS is an Open Source Content Management System, based on PHP, MySQL and the Exponent Framework.					
SQL Injection	29/11/2016	7.5	In framework/modules/core/controllers/expCommentController.php of Exponent CMS 2.4.0, content_id input is passed into showComments. The method showComments is defined in the expCommentControllercontroller with the parameter '$this->params['content_id']' used directly in SQL. Impact is a SQL injection. **Reference: CVE-2016-9481**	NA	A-EXP-EXPON--71216/14
Hdfgroup					
Hdf5 HDF5 is a data model, library, and file format for storing and managing data.					
Overflow	18/11/2016	6.9	The HDF5 1.8.16 library allocating space for the array using a value from the file has an impact within the loop for initializing said array allowing a value within the file to modify the loop's terminator. Due to this, an aggressor can cause the loop's index to point outside the bounds of the array when initializing it. **Reference: CVE-2016-4333**	NA	A-HDF-HDF5--71216/15
Execute Code	18/11/2016	6.9	The library's failure to check if certain message types support a particular flag, the HDF5 1.8.16 library will cast the structure to an alternative structure and then assign to fields that aren't supported by the message type and the library will write	NA	A-HDF-HDF5--71216/16

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

			outside the bounds of the heap buffer. This can lead to code execution under the context of the library. **Reference: CVE-2016-4332**		
Execute Code	18/11/2016	6.9	When decoding data out of a dataset encoded with the H5Z_NBIT decoding, the HDF5 1.8.16 library will fail to ensure that the precision is within the bounds of the size leading to arbitrary code execution. **Reference: CVE-2016-4331**	NA	A-HDF-HDF5--71216/17
Execute Code; Overflow	18/11/2016	6.9	In the HDF5 1.8.16 library's failure to check if the number of dimensions for an array read from the file is within the bounds of the space allocated for it, a heap-based buffer overflow will occur, potentially leading to arbitrary code execution. **Reference: CVE-2016-4330**	NA	A-HDF-HDF5--71216/18
IBM					
Bigfix Remote Control Use IBM BigFix Remote Control to start remote control sessions over the internet with targets that do not have the target software installed.					
NA	25/11/2016	4.3	IBM BigFix Remote Control before 9.1.3 does not properly restrict password choices, which makes it easier for remote attackers to obtain access via a brute-force approach. **Reference: CVE-2016-2929**	http://www-01.ibm.com/support/docview.wss?uid=swg21991880	A-IBM-BIGFI--71216/19
Gain Information	25/11/2016	4	IBM BigFix Remote Control before 9.1.3 allows remote authenticated users to obtain sensitive information by reading error logs. **Reference: CVE-2016-2928**	http://www-01.ibm.com/support/docview.wss?uid=swg21991951	A-IBM-BIGFI--71216/20
Gain Information	25/11/2016	4.3	IBM BigFix Remote Control before 9.1.3 does not properly restrict the set of available	http://www-01.ibm.com/	A-IBM-BIGFI--71216/21

			encryption algorithms, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and performing calculations on encrypted data. **Reference: CVE-2016-2927**	support/docview.wss?uid=swg21991875	
Cross Site Scripting; Cross Site Request Forgery	30/11/2016	6.8	Cross-site request forgery (CSRF) vulnerability in IBM BigFix Remote Control before 9.1.3 allows remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference: CVE-2016-2963**	http://www-01.ibm.com/support/docview.wss?uid=swg21991867	A-IBM-BIGFI--71216/22
Gain Information	30/11/2016	4.3	IBM BigFix Remote Control before 9.1.3 does not enable the HSTS protection mechanism, which makes it easier for remote attackers to obtain sensitive information by leveraging use of HTTP. **Reference: CVE-2016-2952**	http://www-01.ibm.com/support/docview.wss?uid=swg21991871	A-IBM-BIGFI--71216/23
NA	30/11/2016	4.3	IBM BigFix Remote Control before 9.1.3 does not properly set the default encryption strength, which makes it easier for remote attackers to defeat cryptographic protection mechanisms by sniffing the network and performing calculations on encrypted data. **Reference: CVE-2016-2951**	http://www-01.ibm.com/support/docview.wss?uid=swg21991885	A-IBM-BIGFI--71216/24
Execute Code; SQL Injection	30/11/2016	4	SQL injection vulnerability in IBM BigFix Remote Control before 9.1.3 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-2950**	http://www-01.ibm.com/support/docview.wss?uid=swg21991886	A-IBM-BIGFI--71216/25
Gain Information	30/11/2016	2.1	IBM BigFix Remote Control before 9.1.3 allows local users to obtain sensitive information by reading cached web pages	http://www-01.ibm.com/support/doc	A-IBM-BIGFI--71216/26

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

			from a different user's session. **Reference: CVE-2016-2949**	view.wss?uid=swg21991959	
NA	30/11/2016	4.6	IBM BigFix Remote Control before 9.1.3 allows local users to discover hardcoded credentials via unspecified vectors. **Reference: CVE-2016-2948**	http://www-01.ibm.com/support/docview.wss?uid=swg21991889	A-IBM-BIGFI--71216/27
NA	30/11/2016	5	IBM BigFix Remote Control before 9.1.3 does not properly restrict failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force approach. **Reference: CVE-2016-2944**	http://www-01.ibm.com/support/docview.wss?uid=swg21991878	A-IBM-BIGFI--71216/28
Gain Information	30/11/2016	1.9	IBM BigFix Remote Control before 9.1.3 allows local users to obtain sensitive information by leveraging unspecified privileges to read a log file. **Reference: CVE-2016-2943**	http://www-01.ibm.com/support/docview.wss?uid=swg21991960	A-IBM-BIGFI--71216/29
Gain Information	30/11/2016	5	Multiple unspecified vulnerabilities in IBM BigFix Remote Control before 9.1.3 allow remote attackers to obtain sensitive information via unknown vectors. **Reference: CVE-2016-2940**	http://www-01.ibm.com/support/docview.wss?uid=swg21991961	A-IBM-BIGFI--71216/30
Gain Information	30/11/2016	6.4	IBM BigFix Remote Control before 9.1.3 allows remote attackers to obtain sensitive information or spoof e-mail transmission via a crafted POST request, related to an "untrusted information vulnerability." **Reference: CVE-2016-2937**	http://www-01.ibm.com/support/docview.wss?uid=swg21991887	A-IBM-BIGFI--71216/31
Gain Information	30/11/2016	5	IBM BigFix Remote Control before 9.1.3 uses cleartext storage for unspecified passwords, which allows local	http://www-01.ibm.com/support/doc	A-IBM-BIGFI--71216/32

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

			users to obtain sensitive information via unknown vectors. **Reference: CVE-2016-2936**	view.wss?uid=swg21991884	
Denial of Service	30/11/2016	5	The broker application in IBM BigFix Remote Control before 9.1.3 allows remote attackers to cause a denial of service via an invalid HTTP request. **Reference: CVE-2016-2935**	http://www-01.ibm.com/support/docview.wss?uid=swg21991955	A-IBM-BIGFI--71216/33
Cross Site Scripting	30/11/2016	4.3	Cross-site scripting (XSS) vulnerability in IBM BigFix Remote Control before 9.1.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-2934**	http://www-01.ibm.com/support/docview.wss?uid=swg21991870	A-IBM-BIGFI--71216/34
Directory Traversal	30/11/2016	6.8	Directory traversal vulnerability in IBM BigFix Remote Control before 9.1.3 allows remote authenticated administrators to read arbitrary files via a crafted request. **Reference: CVE-2016-2933**	http://www-01.ibm.com/support/docview.wss?uid=swg21991892	A-IBM-BIGFI--71216/35
NA	30/11/2016	5	IBM BigFix Remote Control before 9.1.3 allows remote attackers to conduct XML injection attacks via unspecified vectors. **Reference: CVE-2016-2932**	http://www-01.ibm.com/support/docview.wss?uid=swg21991882	A-IBM-BIGFI--71216/36
Gain Information	30/11/2016	5	IBM BigFix Remote Control before 9.1.3 allows remote attackers to obtain sensitive cleartext information by sniffing the network. **Reference: CVE-2016-2931**	http://www-01.ibm.com/support/docview.wss?uid=swg21991876	A-IBM-BIGFI--71216/37
Connections IBM Connections Suite provides IBM social solutions, including software, real-time social communications and content management capabilities.					
Cross Site Request	30/11/2016	3.5	Cross-site request forgery (CSRF) vulnerability in IBM	http://www-	A-IBM-CONNE--

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

Forgery			Connections 4.0 through CR4, 4.5 through CR5, and 5.0 before CR4 allows remote authenticated users to hijack the authentication of arbitrary users for requests that modify the Connections generic page. **Reference: CVE-2016-3009**	01.ibm.com/support/docview.wss?uid=swg21990864	71216/38
Cross Site Request Forgery	30/11/2016	4.9	Cross-site request forgery (CSRF) vulnerability in IBM Connections 4.0 through CR4, 4.5 through CR5, and 5.0 before CR4 allows remote authenticated users to hijack the authentication of arbitrary users for requests that modify the set of available applications. **Reference: CVE-2016-3004**	http://www-01.ibm.com/support/docview.wss?uid=swg21990864	A-IBM-CONNE--71216/39
Gain Information	30/11/2016	2.1	IBM Connections 4.0 through CR4, 4.5 through CR5, and 5.0 before CR4 allows physically proximate attackers to obtain sensitive information by reading cached data on a client device. **Reference: CVE-2016-3002**	http://www-01.ibm.com/support/docview.wss?uid=swg21990864	A-IBM-CONNE--71216/40
Gain Information	30/11/2016	4	IBM Connections 4.0 through CR4, 4.5 through CR5, and 5.0 before CR4 allows remote authenticated users to obtain sensitive information by reading an "archaic" e-mail address in a response. **Reference: CVE-2016-2958**	http://www-01.ibm.com/support/docview.wss?uid=swg21990864	A-IBM-CONNE--71216/41
Gain Information	30/11/2016	4	IBM Connections 4.0 through CR4, 4.5 through CR5, and 5.0 before CR4 allows remote authenticated users to obtain sensitive information by reading a stack trace in a response. **Reference: CVE-2016-2957**	http://www-01.ibm.com/support/docview.wss?uid=swg21990864	A-IBM-CONNE--71216/42
Gain Information	30/11/2016	4.3	IBM Connections 4.0 through CR4, 4.5 through CR5, and 5.0	http://www-	A-IBM-CONNE--

			before CR4 does not require SSL, which allows remote attackers to obtain sensitive cleartext information by sniffing the network. **Reference: CVE-2016-2953**	01.ibm.com/support/docview.wss?uid=swg21990888	71216/43
Filenet Workplace; Filenet Workplace Xt Workplace XT is an optional FileNet P8 platform component (similar to Application Engine) that hosts the Workplace XT web application, providing access to the process and content functionality of FileNet P8. You can install Workplace XT in addition to or in place of Application Engine. Workplace XT protects user credentials passed between Workplace XT and Content Engine and, if configured, provides SSL security.					
Cross Site Scripting	24/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM FileNet Workplace XT through 1.1.5.2-WPXT-LA011 and FileNet Workplace (Application Engine) through 4.0.2.14-P8AE-IF001, when RegExpSecurityFilter and ScriptSecurityFilter are misconfigured, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5981**	http://www-01.ibm.com/support/docview.wss?uid=swg21990899	A-IBM-FILEN--71216/44
Forms Experience Builder IBM Forms Experience Builder enables line of business users to create web forms applications for stand-alone use or for customer and employee websites.					
Cross Site Scripting; Cross Site Request Forgery	30/11/2016	6	Cross-site request forgery (CSRF) vulnerability in IBM Forms Experience Builder 8.5.x and 8.6.x before 8.6.3.1, in an unspecified non-default configuration, allows remote authenticated users to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference: CVE-2016-2884**	http://www-01.ibm.com/support/docview.wss?uid=swg21987252	A-IBM-FORMS--71216/45
General Parallel File System; Spectrum Scale The General Parallel File System (GPFS) is a high-performance clustered file system developed by IBM; IBM Spectrum Scale is a flexible software-defined storage that can be deployed as high performance file storage or a cost optimized large-scale content repository.					
Gain Privileges	24/11/2016	6.9	IBM Spectrum Scale 4.1.1.x	http://www	A-IBM-

			before 4.1.1.8 and 4.2.x before 4.2.0.4 and General Parallel File System (GPFS) 3.5.x before 3.5.0.32 and 4.1.x before 4.1.1.8 allow local users to gain privileges via crafted environment variables to a /usr/lpp/mmfs/bin/ setuid program. **Reference: CVE-2016-2985**	-01.ibm.com/support/docview.wss?uid=ssg1S1007994	GENER--71216/46
Gain Privileges	24/11/2016	6.9	IBM Spectrum Scale 4.1.1.x before 4.1.1.8 and 4.2.x before 4.2.0.4 and General Parallel File System (GPFS) 3.5.x before 3.5.0.32 and 4.1.x before 4.1.1.8 allow local users to gain privileges via crafted command-line parameters to a /usr/lpp/mmfs/bin/ setuid program. **Reference: CVE-2016-2984**	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1007994	A-IBM-GENER--71216/47
Ims Enterprise Suite IMS Enterprise Suite is a set of components that support open integration technologies to enable new application development and extend access to IMS transactions and data.					
Gain Information	30/11/2016	5.5	IBM IMS Enterprise Suite Data Provider before 3.2.0.1 for Microsoft .NET allows remote authenticated users to obtain sensitive information or modify data via unspecified vectors. **Reference: CVE-2016-2887**	http://www-01.ibm.com/support/docview.wss?uid=swg21982967	A-IBM-IMSE--71216/48
Jazz Reporting Service IBM Jazz Reporting Service is an alternative to the complex reporting capabilities that are available in many Rational products and solutions.					
Denial of Service	25/11/2016	5	The XML parser in Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service 6.0 and 6.0.1 before 6.0.1 iFix006 allows remote authenticated administrators to read arbitrary files or cause a denial of service via an XML document containing an external entity declaration in	http://www-01.ibm.com/support/docview.wss?uid=swg21983137	A-IBM-JAZZ --71216/49

			conjunction with an entity reference, related to an XML External Entity (XXE) issue. **Reference: CVE-2016-0319**		
NA	25/11/2016	6	Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service 6.0 and 6.0.1 before 6.0.1 iFix006 does not destroy a Session ID upon a logout action, which allows remote attackers to obtain access by leveraging an unattended workstation. **Reference: CVE-2016-0318**	http://www-01.ibm.com/support/docview.wss?uid=swg21983137	A-IBM-JAZZ --71216/50
NA	25/11/2016	4.3	Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service 6.0 and 6.0.1 before 6.0.1 iFix006 allows remote attackers to conduct clickjacking attacks via unspecified vectors. **Reference: CVE-2016-0317**	http://www-01.ibm.com/support/docview.wss?uid=swg21983137	A-IBM-JAZZ --71216/51
Cross Site Scripting	25/11/2016	3.5	Cross-site scripting (XSS) vulnerability in Lifecycle Query Engine (LQE) in IBM Jazz Reporting Service 6.0 and 6.0.1 before 6.0.1 iFix006 and 6.0.2 before iFix003 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0316**	http://www-01.ibm.com/support/docview.wss?uid=swg21983137	A-IBM-JAZZ --71216/52
Lotus Inotes IBM iNotes (formerly IBM Lotus iNotes) is a web-based email client for IBM Notes.					
Cross Site Scripting	24/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM iNotes before 8.5.3 FP6 IF2 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL, aka SPR KLYHAAHNUS. **Reference: CVE-2016-0282**	http://www-01.ibm.com/support/docview.wss?uid=swg21991722	A-IBM-LOTUS--71216/53
Maximo Asset Management IBM Maximo Asset Management is an enterprise asset management (EAM) software solution product produced by IBM.					

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	30/11/2016	5	IBM Maximo Asset Management 7.1 through 7.1.1.13, 7.5 before 7.5.0.10 IF4, and 7.6 before 7.6.0.5 IF3 allows remote attackers to obtain sensitive information via a crafted HTTP request that triggers construction of a runtime error message. **Reference: CVE-2016-5987**	http://www-01.ibm.com/support/docview.wss?uid=swg21990449	A-IBM-MAXIM--71216/54
Cross Site Scripting	30/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM Maximo Asset Management 7.5 before 7.5.0.10 IF3 and 7.6 before 7.6.0.5 IF2 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5905**	http://www-01.ibm.com/support/docview.wss?uid=swg21988253	A-IBM-MAXIM--71216/55
Qradar Security Information And Event Manager IBM QRadar SIEM consolidates log events and network flow data from thousands of devices, endpoints and applications distributed throughout a network.					
Bypass	30/11/2016	6.4	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 and QRadar Incident Forensics 7.2 before 7.2.7 allow remote attackers to bypass intended access restrictions via modified request parameters. **Reference: CVE-2016-2881**	http://www-01.ibm.com/support/docview.wss?uid=swg21987777	A-IBM-QRADA--71216/56
Cross Site Scripting; Cross Site Request Forgery	30/11/2016	6	Multiple cross-site request forgery (CSRF) vulnerabilities in IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 allow remote attackers to hijack the authentication of arbitrary users for requests that insert XSS sequences. **Reference: CVE-2016-2878**	http://www-01.ibm.com/support/docview.wss?uid=swg21987776	A-IBM-QRADA--71216/57
NA	30/11/2016	2.1	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 uses weak permissions for unspecified directories under the web root, which	http://www-01.ibm.com/support/docview.wss?ui	A-IBM-QRADA--71216/58

			allows local users to modify data by writing to a file. **Reference: CVE-2016-2877**	d=swg2198 7773	
Execute Code	30/11/2016	8.5	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 executes unspecified processes at an incorrect privilege level, which makes it easier for remote authenticated users to obtain root access by leveraging a command-injection issue. **Reference: CVE-2016-2876**	http://www-01.ibm.com/support/docview.wss?uid=swg2198 7774	A-IBM-QRADA--71216/59
Gain Information	30/11/2016	3.5	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 mishandles authorization, which allows remote authenticated users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-2874**	http://www-01.ibm.com/support/docview.wss?uid=swg2198 7771	A-IBM-QRADA--71216/60
Execute Code; SQL Injection	30/11/2016	6.5	SQL injection vulnerability in IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **Reference: CVE-2016-2873**	http://www-01.ibm.com/support/docview.wss?uid=swg2198 7770	A-IBM-QRADA--71216/61
Gain Information	30/11/2016	4.6	IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 uses cleartext storage for unspecified passwords, which allows local users to obtain sensitive information by reading a configuration file. **Reference: CVE-2016-2871**	http://www-01.ibm.com/support/docview.wss?uid=swg2198 7769	A-IBM-QRADA--71216/62
Cross Site Scripting	30/11/2016	3.5	Multiple cross-site scripting (XSS) vulnerabilities in the UI in IBM QRadar SIEM 7.1 before MR2 Patch 13 and 7.2 before 7.2.7 allow remote authenticated users to inject arbitrary web script or HTML via crafted fields in a URL.	http://www-01.ibm.com/support/docview.wss?uid=swg2198 7768	A-IBM-QRADA--71216/63

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-2016-2869		
Rational Asset Analyzer IBM Rational Asset Analyzer collects and analyzes information about software applications.					
NA	24/11/2016	2.1	The installation component in IBM Rational Asset Analyzer (RAA) 6.1.0 before FP10 allows local users to discover the WAS Admin password by reading IM native logs. **Reference: CVE-2016-5967**	http://www-01.ibm.com/support/docview.wss?uid=swg21990215	A-IBM-RATIO--71216/64
Rational Collaborative Lifecycle Management; Rational Doors Next Generation; Rational Engineering Lifecycle Manager; Rational Quality Manager; Rational Rhapsody Design Manager; Rational Software Architect Design Manager; Rational Team Concert The IBM Rational solution for Collaborative Lifecycle Management (CLM) brings together requirements management, quality management, change and configuration management, project planning and tracking on a common unified platform; Rational DOORS Next Generation (RDNG) is a web-based requirements management tool developed as part of Collaborative Lifecycle Management (in the Jazz Requirement Management application) to empower teams to define, manage, and report on requirements in complex systems and software engineering environments; IBM Rational Engineering Lifecycle Manager visualizes, analyzes and organizes engineering lifecycle data and data relationships; Rational Quality Manager is a test management tool which stores test cases, records test execution and results, maps testing onto requirements and tracks defects; IBM Rational Rhapsody Design Manager is collaborative design management software that helps design teams and their stakeholders to share, trace, review and manage designs; IBM Rational Software Architect Design Manager is a collaborative software design and development platform built on Jazz technology; Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008, which is available in both client versions and a Web version.					
Gain Information	24/11/2016	4	IBM Rational Collaborative Lifecycle Management 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Quality Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before	http://www-01.ibm.com/support/docview.wss?uid=swg21991477	A-IBM-RATIO--71216/65

			4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 allow remote authenticated users to obtain sensitive information via unspecified vectors. **Reference: CVE-2016-2947**		
Cross Site Scripting	2016-11-24	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18,	http://www-01.ibm.com/support/docview.wss?uid=swg21991478	A-IBM-RATIO--71216/66

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

			and 6.0 before 6.0.2 iFix5 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-2864**		
NA	2016-11-24	4.3	IBM Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 do 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-2016-0372**	http://www-01.ibm.com/support/docview.wss?uid=swg21991478	A-IBM-RATIO--71216/67
Denial of Service	24/11/2016	5.5	The XML parser in IBM Rational Collaborative	http://www-	A-IBM-RATIO--

			Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 allows remote authenticated users to read arbitrary files or cause a denial of service 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-2016-0284**	01.ibm.com/support/docview.wss?uid=swg21991478	71216/68
Cross Site Scripting	2016-11-24	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational	http://www-01.ibm.com/support/docview.wss?uid=swg21991478	A-IBM-RATIO--71216/69

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

			Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-0273**		
Cross Site Scripting	2016-11-25	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3; Rational Quality Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3; Rational Team Concert 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before	http://www-01.ibm.com/support/docview.wss?uid=swg21993444	A-IBM-RATIO--71216/70

			6.0.2 iFix3; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix19, and 6.0 before 6.0.2 iFix3 allows remote authenticated users to inject arbitrary web script or HTML via a crafted URL. **Reference: CVE-2016-2926**		
Cross Site Scripting	30/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, Rational Quality Manager 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, Rational Team Concert 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, Rational DOORS Next Generation 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17, and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11 and 5.0 before 5.0.2 iFix17 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	http://www-01.ibm.com/support/docview.wss?uid=swg21992151	A-IBM-RATIO--71216/71

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-2016-3014		
Rational Doors Next Generation Rational Doors Next Generation (RDNG) is a web-based requirements management tool developed as part of Collaborative Lifecycle Management (in the Jazz Requirement Management application) to empower teams to define, manage, and report on requirements in complex systems and software engineering environments.					
Cross Site Scripting	24/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational DOORS Next Generation 6.0.2 before iFix004 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-5955**	http://www-01.ibm.com/support/docview.wss?uid=swg21990054	A-IBM-RATIO--71216/72
Rational Doors Next Generation; Rational Engineering Lifecycle Manager; Rational Quality Manager; Rational Rhapsody Design Manager; Rational Team Concert Rational DOORS Next Generation (RDNG) is a web-based requirements management tool developed as part of Collaborative Lifecycle Management (in the Jazz Requirement Management application) to empowers teams to define, manage, and report on requirements in complex systems and software engineering environments; IBM Rational Engineering Lifecycle Manager visualizes, analyzes and organizes engineering lifecycle data and data relationships ; Rational Quality Manager is a test management tool which stores test cases, records test execution and results, maps testing onto requirements and tracks defects; IBM Rational Rhapsody Design Manager is collaborative design management software that helps design teams and their stakeholders to share, trace, review and manage designs; Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008, which is available in both client versions and a Web version					
Cross Site Scripting	2016-11-24	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 6.x before 6.0.1 iFix6, Rational Quality Manager 6.x before 6.0.1 iFix6, Rational Team Concert 6.x before 6.0.1 iFix6, Rational DOORS Next Generation 6.x before 6.0.1 iFix6, Rational Engineering Lifecycle Manager 6.x before 6.0.1 iFix6, and Rational Rhapsody Design Manager 6.x before 6.0.1 iFix6 allows remote authenticated users to inject arbitrary web script or HTML via unspecified vectors.	http://www-01.ibm.com/support/docview.wss?uid=swg21989940	A-IBM-RATIO--71216/73

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-2016-2986		
Rational Team Concert Rational Team Concert is a software development team collaboration tool developed by the Rational Software brand of IBM, who first released it in 2008.					
Execute Code	24/11/2016	7.5	IBM Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 allow remote authenticated users to execute arbitrary OS commands via a crafted request. **Reference: CVE-2016-0325**	http://www-01.ibm.com/support/docview.wss?uid=swg21991478	A-IBM-RATIO--71216/74
Cross Site Scripting	24/11/2016	3.5	Cross-site scripting (XSS) vulnerability in IBM Rational Collaborative Lifecycle Management 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational	http://www-01.ibm.com/support/docview.wss?uid=swg21991478	A-IBM-RATIO--71216/75

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

			Quality Manager 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Team Concert 3.0.1.6 before iFix8, 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational DOORS Next Generation 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Engineering Lifecycle Manager 4.x before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; Rational Rhapsody Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5; and Rational Software Architect Design Manager 4.0 before 4.0.7 iFix11, 5.0 before 5.0.2 iFix18, and 6.0 before 6.0.2 iFix5 allows remote authenticated users to inject arbitrary web script or HTML via a crafted field. **Reference: CVE-2016-0285**		
Security Access Manager; Security Access Manager For Mobile IBM Security Access Manager integrated appliance is designed to manage access in the world of Hybrid Cloud and enable SSO and identity federation to apps running inside & outside of the enterprise; IBM Security Access Manager enables businesses to more securely adopt web, mobile, and cloud technologies and simplifies user access management for employees and consumers.					
NA	24/11/2016	5	IBM Security Access Manager for Mobile 8.x before 8.0.1.4 IF3 and Security Access Manager 9.x before 9.0.1.0 IF5 do not properly restrict failed login attempts, which makes it easier for remote attackers to obtain access via a brute-force approach. **Reference: CVE-2016-3025**	http://www-01.ibm.com/support/docview.wss?uid=swg21991107	A-IBM-SECUR--71216/76
Security Access Manager; Security Access Manager For Web					

IBM Security Access Manager integrated appliance is designed to manage access in the world of Hybrid Cloud and enable SSO and identity federation to apps running inside & outside of the enterprise; IBM Security Access Manager enables businesses to more securely adopt web, mobile, and cloud technologies and simplifies user access management for employees and consumers.					
Execute Code	24/11/2016	9	IBM Security Access Manager for Web 7.0 before IF2 and 8.0 before 8.0.1.4 IF3 and Security Access Manager 9.0 before 9.0.1.0 IF5 allow remote authenticated users to execute arbitrary commands by leveraging LMI admin access. **Reference: CVE-2016-3028**	http://www-01.ibm.com/support/docview.wss?uid=swg21990317	A-IBM-SECUR--71216/77
Security Privileged Identity Manager IBM Security Privileged Identity Manager helps organizations manage, automate, and track the use of shared privileged identities.					
NA	24/11/2016	4	IBM Security Privileged Identity Manager 2.0 before 2.0.2 FP8, when Virtual Appliance is used, allows remote authenticated users to append to arbitrary files via unspecified vectors. **Reference: CVE-2016-2996**	http://www-01.ibm.com/support/docview.wss?uid=swg21988706	A-IBM-SECUR--71216/78
NA	24/11/2016	4.3	IBM Security Privileged Identity Manager 2.0 before 2.0.2 FP8, when Virtual Appliance is used, 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-2016-0353**	http://www-01.ibm.com/support/docview.wss?uid=swg21988706	A-IBM-SECUR--71216/79
Sterling B2b Integrator IBM Sterling B2B Integrator enables the security-rich integration of complex B2B processes with diverse partner communities.					
NA	30/11/2016	3.5	IBM Sterling B2B Integrator 5.2 before 5020500_14 and 5.2 06 before 5020602_1 allows remote authenticated users to change arbitrary passwords via unspecified	http://www-01.ibm.com/support/docview.wss?uid=swg2198	A-IBM-STERL--71216/80

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

			vectors. **Reference: CVE-2016-5890**	9577	
Cross Site Scripting	30/11/2016	4.3	Cross-site scripting (XSS) vulnerability in IBM Sterling B2B Integrator 5.2 before 5020500_14 and 5.2 06 before 5020602_1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **Reference: CVE-2016-3057**	http://www-01.ibm.com/support/docview.wss?uid=swg21989578	A-IBM-STERL--71216/81
Sterling Connect IBM Sterling Connect Direct offers a variety of capabilities for billing, secure transfer of sensitive information, and the synchronization of data-recovery.					
Denial of Service	24/11/2016	1.9	IBM Sterling Connect:Direct 4.5.00, 4.5.01, 4.6.0 before 4.6.0.6 iFix008, and 4.7.0 before 4.7.0.4 on Windows allows local users to cause a denial of service via unspecified vectors. **Reference: CVE-2016-5992**	http://www-01.ibm.com/support/docview.wss?uid=swg21989807	A-IBM-STERL--71216/82
Gain Privileges	24/11/2016	4.4	IBM Sterling Connect:Direct 4.5.00, 4.5.01, 4.6.0 before 4.6.0.6 iFix008, and 4.7.0 before 4.7.0.4 on Windows allows local users to gain privileges via unspecified vectors. **Reference: CVE-2016-5991**	http://www-01.ibm.com/support/docview.wss?uid=swg21989807	A-IBM-STERL--71216/83
Tealeaf Customer Experience IBM Tealeaf customer experience management solutions provide visibility and insight to help meet online conversion and customer retention objectives.					
NA	24/11/2016	5	The Replay Server in IBM Tealeaf Customer Experience 8.x before 8.7.1.8847 FP10, 8.8.x 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 FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224 FP3 allows remote attackers to conduct SSRF attacks via unspecified vectors.	http://www-01.ibm.com/support/docview.wss?uid=swg21989374	A-IBM-TEALE--71216/84

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-2016-5968		
Tealeaf Customer Experience IBM Tealeaf customer experience management solutions provide visibility and insight to help meet online conversion and customer retention objectives.					
Gain Information	24/11/2016	2.9	IBM Tealeaf Customer Experience 8.x before 8.7.1.8847 FP10, 8.8.x 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 FP5, 9.0.2 before 9.0.2.1223 FP3, and 9.0.2A before 9.0.2.5224 FP3 does not encrypt connections between internal servers, which allows remote attackers to obtain sensitive information by sniffing the network for HTTP traffic. **Reference: CVE-2015-4961**	http://www-01.ibm.com/support/docview.wss?uid=swg21965077	A-IBM-TEALE--71216/85
Tivoli Storage Manager For Virtual Environments IBM Tivoli Storage Manager for Virtual Environments: Data Protection for VMware provides a comprehensive solution for protecting VMs.					
Bypass	24/11/2016	4.6	IBM Tivoli Storage Manger for Virtual Environments: Data Protection for VMware (aka Spectrum Protect for Virtual Environments) 6.4.x before 6.4.3.4 and 7.1.x before 7.1.6 allows remote authenticated users to bypass a TSM credential requirement and obtain administrative access by leveraging multiple simultaneous logins. **Reference: CVE-2016-2988**	http://www-01.ibm.com/support/docview.wss?uid=swg21988781	A-IBM-TIVOL--71216/86
Tririga Application Platform IBM TRIRIGA Application Platform provides a single web-based set of design-time and runtime components.					
Gain Privileges; Gain Information	30/11/2016	6.5	The notifications component in IBM TRIRIGA Applications 10.4 and 10.5 before 10.5.1 allows remote authenticated users to obtain sensitive password information, and consequently gain privileges,	http://www-01.ibm.com/support/docview.wss?uid=swg21984304	A-IBM-TRIRI--71216/87

			via unspecified vectors. **Reference: CVE-2016-2917**		
Websphere Application Server WebSphere Application Server (WAS) is a software product that performs the role of a web application server.					
Gain Information	24/11/2016	4.3	IBM WebSphere Application Server (WAS) Liberty before 16.0.0.3, when the installation lacks a default error page, allows remote attackers to obtain sensitive information by triggering an exception. **Reference: CVE-2016-0378**	http://www-01.ibm.com/support/docview.wss?uid=swg21981529	A-IBM-WEBSP--71216/88
Libdwarf Project					
Libdwarf Libdwarf is a C library intended to simplify reading (and writing) applications using DWARF2, DWARF3.					
Denial of Service; Overflow; Gain Information	29/11/2016	6.4	libdwarf 2016-10-21 allows context-dependent attackers to obtain sensitive information or cause a denial of service by using the "malformed dwarf file" approach, related to a "Heap Buffer Over-read" issue affecting the dwarf_util.c component, aka DW201611-006. **Reference: CVE-2016-9480**	https://sourceforge.net/p/libdwarf/bugs/5/	A-LIB-LIBDW--71216/89
Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
Overflow	22/11/2016	7.5	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka "cpStripToTile heap-buffer-overflow." **Reference: CVE-2016-9540**	https://github.com/vadz/libtiff/commit/5ad9d8016fbb60109302d558f7edb2cb2a3bb8e3	A-LIB-LIBTI--71216/90
NA	22/11/2016	7.5	tools/tiffcrop.c in libtiff 4.0.6 has an out-of-bounds read in readContigTilesIntoBuffer(). Reported as MSVR 35092. **Reference: CVE-2016-9539**	https://github.com/vadz/libtiff/commit/ae9365db1b271b	A-LIB-LIBTI--71216/91

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

				62b35ce018eac8799b1d5e8a53	
Overflow	22/11/2016	7.5	tools/tiffcrop.c in libtiff 4.0.6 reads an undefined buffer in readContigStripsIntoBuffer() because of a uint16 integer overflow. Reported as MSVR 35100. **Reference: CVE-2016-9538**	https://github.com/vadz/libtiff/commit/43c0b81a818640429317c80fea1e66771e85024b#diff-c8b4b355f9b5c06d585b23138e1c185f	A-LIB-LIBTI--71216/92
NA	22/11/2016	7.5	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097. **Reference: CVE-2016-9537**	https://github.com/vadz/libtiff/commit/83a4b92815ea04969d494416eaae3d4c6b338e4a#diff-c8b4b355f9b5c06d585b23138e1c185f	A-LIB-LIBTI--71216/93
Overflow	22/11/2016	7.5	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka "t2p_process_jpeg_strip heap-buffer-overflow." **Reference: CVE-2016-9536**	https://github.com/vadz/libtiff/commit/83a4b92815ea04969d494416eaae3d4c6b338e4a#diff-5173a9b3b48146e4fd86d7b9b346115e	A-LIB-LIBTI--71216/94
Overflow	22/11/2016	7.5	tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with	https://github.com/vadz/libtiff/commit/3ca657a8793dd011bf869695d	A-LIB-LIBTI--71216/95

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

			unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka "Predictor heap-buffer-overflow." **Reference: CVE-2016-9535**	72ad31c779c3cc1	
Overflow	22/11/2016	7.5	tif_write.c in libtiff 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aka "TIFFFlushData1 heap-buffer-overflow." **Reference: CVE-2016-9534**	https://github.com/vadz/libtiff/commit/83a4b92815ea04969d494416eaae3d4c6b338e4a#diff-5be5ce02d0dea67050d5b2a10102d1ba	A-LIB-LIBTI--71216/96
Overflow	22/11/2016	7.5	tif_pixarlog.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "PixarLog horizontalDifference heap-buffer-overflow." **Reference: CVE-2016-9533**	https://github.com/vadz/libtiff/commit/83a4b92815ea04969d494416eaae3d4c6b338e4a#diff-bdc795f6afeb9558c1012b3cfae729ef	A-LIB-LIBTI--71216/97
Microfocus					
Host Access Management And Security Server; Reflection For The Web; Reflection Security Gateway; Reflection Zfe Micro Focus Host Access Management and Security Server improves your security while centralizing host system control using legacy resources; Deliver zero-footprint, HTML5-based terminal emulation that you can manage from a browser with Micro Focus Reflection ZFE.					
Directory Traversal	29/11/2016	4.3	Administrative Server in Micro Focus Host Access Management and Security Server (MSS) and Reflection for the Web (RWeb) and Reflection Security Gateway (RSG) and Reflection ZFE (ZFE) allows remote unauthenticated attackers to read arbitrary files via a	http://support.attachmate.com/techdocs/1704.html	A-MIC-HOST --71216/98

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

			specially crafted URL that allows limited directory traversal. Applies to MSS 12.3 before 12.3.326 and MSS 12.2 before 12.2.342 and RSG 12.1 before 12.1.362 and RWeb 12.3 before 12.3.312 and RWeb 12.2 before 12.2.342 and RWeb 12.1 before 12.1.362 and ZFE 2.0.1 before 2.0.1.18 and ZFE 2.0.0 before 2.0.0.52 and ZFE 1.4.0 before 1.4.0.14. **Reference: CVE-2016-5765**		
Nginx					
Nginx NGINX is one of a handful of servers written to address the C10K problem.					
Gain Privileges	29/11/2016	7.2	The nginx package before 1.6.2-5+deb8u3 on Debian jessie and the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10 allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log. **Reference: CVE-2016-1247**	NA	A-NGI-NGINX--71216/99
SAP					
Netweaver SAP NetWeaver is the primary technology computing platform of the software company SAP SE, and the technical foundation for many SAP applications.					
NA	22/11/2016	6	BC-BMT-BPM-DSK in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to conduct XML External Entity (XXE) attacks via the sap.com~tc~bpem~him~uwlconn~provider~web/bpemuwlconn URI, aka SAP Security Note 2296909.	NA	A-SAP-NETWE--71216/100

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-2016-9563		
Denial of Service	22/11/2016	5	SAP NetWeaver AS JAVA 7.4 allows remote attackers to cause a Denial of Service (null pointer exception and icman outage) via an HTTPS request to the sap.com~P4TunnelingApp!web/myServlet URI, aka SAP Security Note 2313835. **Reference: CVE-2016-9562**	NA	A-SAP-NETWE--71216/101
Soap					
NA	22/11/2016	5	In Soap Lite (aka the SOAP::Lite extension for Perl) 1.14 and earlier, an example attack consists of defining 10 or more XML entities, each defined as consisting of 10 of the previous entity, with the document consisting of a single instance of the largest entity, which expands to one billion copies of the first entity. The amount of computer memory used for handling an external SOAP call would likely exceed that available to the process parsing the XML. **Reference: CVE-2015-8978**	http://cpansearch.perl.org/src/PHRED/SOAP-Lite-1.20/Changes	A-SOA-NA--71216/102
Wireshark					
Wireshark Wireshark is a network protocol analyzer for Unix and Windows.					
NA	17/11/2016	4.3	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the OpenFlow dissector could crash with memory exhaustion, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-openflow_v5.c by ensuring that certain length values were sufficiently large. **Reference: CVE-2016-9376**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13071	A-WIR-WIRES--71216/103

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

NA	17/11/2016	4.3	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the DTN dissector could go into an infinite loop, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-dtn.c by checking whether SDNV evaluation was successful. **Reference: CVE-2016-9375**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13097	A-WIR-WIRES--71216/104
Overflow	17/11/2016	4.3	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the AllJoyn dissector could crash with a buffer over-read, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-alljoyn.c by ensuring that a length variable properly tracked the state of a signature variable. **Reference: CVE-2016-9374**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12953	A-WIR-WIRES--71216/105
NA	17/11/2016	4.3	In Wireshark 2.2.0 to 2.2.1 and 2.0.0 to 2.0.7, the DCERPC dissector could crash with a use-after-free, triggered by network traffic or a capture file. This was addressed in epan/dissectors/packet-dcerpc-nt.c and epan/dissectors/packet-dcerpc-spoolss.c by using the wmem file scope for private strings. **Reference: CVE-2016-9373**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=13072	A-WIR-WIRES--71216/106
NA	17/11/2016	4.3	In Wireshark 2.2.0 to 2.2.1, the Profinet I/O dissector could loop excessively, triggered by network traffic or a capture file. This was addressed in plugins/profinet/packet-pn-rtc-one.c by rejecting input with too many I/O objects. **Reference: CVE-2016-9372**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12851	A-WIR-WIRES--71216/107

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

Application; Operating System (A/OS)					
Debian/VIM					
Debian Linux/VIM Debian is an operating system and a distribution of Free Software/ VIM is an editor to create or edit a text file. There are two modes in vim-one is the command mode and another is the insert mode. In the command mode, user can move around the file, delete text, etc.					
Execute Code	23/11/2016	6.8	Vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened. **Reference: CVE-2016-1248**	http://openwall.com/lists/oss-security/2016/11/22/20	A-OS-DEB-DEBIA--71216/108
Operating System (OS)					
Canonical; Linux					
Ubuntu Linux/Linux Kernel Ubuntu is a Debian-based Linux operating system and distribution for personal computers, smartphones and network servers. It uses Unity as its default desktop environment/ The Linux kernel is a monolithic Unix-like computer operating system kernel.					
NA	27/11/2016	7.2	The overlayfs implementation in the linux (aka Linux kernel) package before 3.19.0-21.21 in Ubuntu through 15.04 does not properly check permissions for file creation in the upper filesystem directory, which allows local users to obtain root access by leveraging a configuration in which overlayfs is permitted in an arbitrary mount namespace. **Reference: CVE-2015-1328**	https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-1328.html	O-CAN-UBUNT--71216/109
Cisco					
Email Security Appliance Firmware NA					
Bypass	18/11/2016	5	A vulnerability in the email filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/c	O-CIS-EMAIL--71216/110

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

			attacker to bypass Advanced Malware Protection (AMP) filters that are configured for an affected device. This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for both virtual and hardware versions of Cisco Email Security Appliances, if the AMP feature is configured to scan incoming email attachments. More Information: CSCuz85823. Known Affected Releases: 10.0.0-082 9.7.0-125 9.7.1-066. Known Fixed Releases: 10.0.0-203 9.7.2-131. **Reference: CVE-2016-6463**	isco-sa-20161116-esa2	
Bypass	18/11/2016	5	A vulnerability in the email filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to bypass Advanced Malware Protection (AMP) filters that are configured for an affected device. This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for both virtual and hardware versions of Cisco Email Security Appliances, if the AMP feature is configured to scan incoming email attachments. More Information: CSCva13456. Known Affected Releases: 10.0.0-082 10.0.0-125 9.7.1-066. Known Fixed Releases: 10.0.0-203 9.7.2-131. **Reference: CVE-2016-6462**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161116-esa1	O-CIS-EMAIL--71216/111
Bypass	18/11/2016	5	A vulnerability in the content	https://tool	O-CIS-

			filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances could allow an unauthenticated, remote attacker to bypass content filters configured on an affected device. Email that should have been filtered could instead be forwarded by the device. This vulnerability affects all releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances, if the software is configured to use a content filter for email attachments that are protected or encrypted. More Information: CSCva52546. Known Affected Releases: 10.0.0-125 9.7.1-066. **Reference: CVE-2016-6458**	s.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-esa	EMAIL--71216/112
IOS XE IOS XE is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), introduced with the ASR 1000 series.					
NA	18/11/2016	1.9	A vulnerability in the package unbundle utility of Cisco IOS XE Software could allow an authenticated, local attacker to gain write access to some files in the underlying operating system. This vulnerability affects the following products if they are running a vulnerable release of Cisco IOS XE Software: Cisco 5700 Series Wireless LAN Controllers, Cisco Catalyst 3650 Series Switches, Cisco Catalyst 3850 Series Switches, Cisco Catalyst 4500E Series Switches, Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161115-iosxe	O-CIS-IOSX--71216/113

			Catalyst 4500X Series Switches. More Information: CSCva60013 CSCvb22622. Known Affected Releases: 3.7(0) 16.4.1 Denali-16.1.3 Denali-16.2.2 Denali-16.3.1. Known Fixed Releases: 15.2(4)E3 16.1(2.208) 16.2(2.42) 16.3(1.22) 16.4(0.190) 16.5(0.29). **Reference: CVE-2016-6450**		
Dell					
Idrac7 Firmware; Idrac8 Firmware NA					
NA	29/11/2016	9	Dell iDRAC7 and iDRAC8 devices with firmware before 2.40.40.40 allow authenticated users to gain Bash shell access through a string injection. **Reference: CVE-2016-5685**	NA	O-DEL-IDRAC--71216/114
GE					
Bently Nevada 3500/22m Serial Firmware; Bently Nevada 3500/22m Usb Firmware GE's Bently Nevada 3500 Monitoring System provides continuous, online monitoring suitable for machinery protection and asset condition monitoring applications.					
NA	24/11/2016	10	General Electric (GE) Bently Nevada 3500/22M USB with firmware before 5.0 and Bently Nevada 3500/22M Serial have open ports, which makes it easier for remote attackers to obtain privileged access via unspecified vectors. **Reference: CVE-2016-5788**	NA	O-GE-BENTL--71216/115
Google					
Android Android is an OS created by Google for use on mobile devices, such as smart-phones and tablets.					
Execute Code	25/11/2016	6.8	A remote code execution vulnerability in Webview in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-11-05 could enable a remote attacker to execute arbitrary code when	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/116

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

			the user is navigating to a website. This issue is rated as High due to the possibility of remote code execution in an unprivileged process. Android ID: A-31217937. **Reference: CVE-2016-6754**		
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in kernel components, including the process-grouping subsystem and the networking subsystem, in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30149174. **Reference: CVE-2016-6753**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/117
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-31498159. References: Qualcomm QC-CR#987051. **Reference: CVE-2016-6752**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/118
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/119

			before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30902162. References: Qualcomm QC-CR#1062271. **Reference: CVE-2016-6751**		
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30312054. References: Qualcomm QC-CR#1052825. **Reference: CVE-2016-6750**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/120
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30228438. References: Qualcomm QC-CR#1052818. **Reference: CVE-2016-6749**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/121

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	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30076504. References: Qualcomm QC-CR#987018. **Reference: CVE-2016-6748**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/122
Denial of Service	25/11/2016	7.1	A denial of service vulnerability in Mediaserver in Android before 2016-11-05 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-31244612. References: NVIDIA N-CVE-2016-6747. **Reference: CVE-2016-6747**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/123
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Android ID: A-30955105. References: NVIDIA N-CVE-2016-6746. **Reference: CVE-2016-6746**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/124
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Synaptics	https://source.android.c	O-GOO-ANDRO--

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

			touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-31252388. **Reference: CVE-2016-6745**	om/security /bulletin/20 16-11- 01.html	71216/ 125
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30970485. **Reference: CVE-2016-6744**	https://sour ce.android.c om/security /bulletin/20 16-11- 01.html	O-GOO- ANDRO-- 71216/ 126
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30937462. **Reference: CVE-2016-6743**	https://sour ce.android.c om/security /bulletin/20 16-11- 01.html	O-GOO- ANDRO-- 71216/ 127
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Synaptics touchscreen driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This	https://sour ce.android.c om/security /bulletin/20 16-11- 01.html	O-GOO- ANDRO-- 71216/ 128

			issue is rated as High because it first requires compromising a privileged process. Android ID: A-30799828. **Reference: CVE-2016-6742**		
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30559423. References: Qualcomm QC-CR#1060554. **Reference: CVE-2016-6741**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/129
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30143904. References: Qualcomm QC-CR#1056307. **Reference: CVE-2016-6740**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/130
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Qualcomm camera driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30074605. References:	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/131

			Qualcomm QC-CR#1049826. **Reference: CVE-2016-6739**		
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Qualcomm crypto engine driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30034511. References: Qualcomm QC-CR#1050538. **Reference: CVE-2016-6738**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/132
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the kernel ION subsystem in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30928456. **Reference: CVE-2016-6737**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/133
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/134

			operating system to repair the device. Android ID: A-30953284. References: NVIDIA N-CVE-2016-6736. **Reference: CVE-2016-6736**		
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30907701. References: NVIDIA N-CVE-2016-6735. **Reference: CVE-2016-6735**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/135
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30907120. References: NVIDIA N-CVE-2016-6734. **Reference: CVE-2016-6734**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/136
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/137

			the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906694. References: NVIDIA N-CVE-2016-6733. **Reference: CVE-2016-6733**		
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906599. References: NVIDIA N-CVE-2016-6732. **Reference: CVE-2016-6732**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/138
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30906023. References: NVIDIA N-CVE-2016-6731. **Reference: CVE-2016-6731**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/139

Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the NVIDIA GPU driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30904789. References: NVIDIA N-CVE-2016-6730. **Reference: CVE-2016-6730**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/140
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the Qualcomm bootloader in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30977990. References: Qualcomm QC-CR#977684. **Reference: CVE-2016-6729**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/141
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in the kernel ION subsystem in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/142

			compromise, which may require reflashing the operating system to repair the device. Android ID: A-30400942. **Reference: CVE-2016-6728**		
Execute Code	25/11/2016	10	A remote code execution vulnerability in the Qualcomm crypto driver in Android before 2016-11-05 could enable a remote attacker to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of remote code execution in the context of the kernel. Android ID: A-30515053. References: Qualcomm QC-CR#1050970. **Reference: CVE-2016-6725**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/143
Denial of Service	25/11/2016	7.1	A denial of service vulnerability in the Input Manager Service in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to cause the device to continually reboot. This issue is rated as Moderate because it is a temporary denial of service that requires a factory reset to fix. Android ID: A-30568284. **Reference: CVE-2016-6724**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/144
Denial of Service	25/11/2016	5.4	A denial of service vulnerability in Proxy Auto Config in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a remote attacker to use a specially crafted file to cause a device	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/145

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

			hang or reboot. This issue is rated as Moderate because it requires an uncommon device configuration. Android ID: A-30100884. **Reference: CVE-2016-6723**		
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Mediaserver in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Android ID: A-30875060. **Reference: CVE-2016-6721**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/146
Bypass	25/11/2016	4.3	An elevation of privilege vulnerability in the Bluetooth component in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to pair with any Bluetooth device without user consent. This issue is rated as Moderate because it is a local bypass of user interaction requirements (access to functionality that would normally require either user initiation or user permission.) Android ID: A-29043989. **Reference: CVE-2016-6719**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/147
Bypass; Gain Information	25/11/2016	4.3	An elevation of privilege vulnerability in the Account Manager Service in Android 7.0 before 2016-11-01 could enable a local malicious application to retrieve	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/148

			sensitive information without user interaction. This issue is rated as Moderate because it is a local bypass of user interaction requirements (access to functionality that would normally require either user initiation or user permission.) Android ID: A-30455516. **Reference: CVE-2016-6718**		
Execute Code	25/11/2016	7.6	An elevation of privilege vulnerability in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Moderate because it first requires exploitation of a separate vulnerability. Android ID: A-31350239. **Reference: CVE-2016-6717**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/149
Bypass	25/11/2016	4.3	An elevation of privilege vulnerability in the AOSP Launcher in Android 7.0 before 2016-11-01 could allow a local malicious application to create shortcuts that have elevated privileges without the user's consent. This issue is rated as Moderate because it is a local bypass of user interaction requirements (access to functionality that would normally require either user initiation or user permission). Android ID: A-30778130. **Reference: CVE-2016-6716**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/150
Bypass	25/11/2016	4.3	An elevation of privilege	https://sour	O-GOO-

			vulnerability in the Framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could allow a local malicious application to record audio without the user's permission. This issue is rated as Moderate because it is a local bypass of user interaction requirements (access to functionality that would normally require either user initiation or user permission.) Android ID: A-29833954. **Reference: CVE-2016-6715**	ce.android.com/security/bulletin/2016-11-01.html	ANDRO--71216/151
Denial of Service	25/11/2016	7.1	A remote denial of service vulnerability in Mediaserver in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-31092462. **Reference: CVE-2016-6714**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/152
Denial of Service	25/11/2016	7.1	A remote denial of service vulnerability in Mediaserver in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Android ID: A-30822755. **Reference: CVE-2016-6713**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/153
Bypass; Gain	25/11/2016	4.3	An information disclosure	https://sour	O-GOO-

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

Information			vulnerability in the download manager in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Android ID: A-30537115. **Reference: CVE-2016-6710**	ce.android.com/security/bulletin/2016-11-01.html	ANDRO--71216/154
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Conscrypt and BoringSSL in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable a man-in-the-middle attacker to gain access to sensitive information if a non-standard cipher suite is used by an application. This issue is rated as High because it could be used to access data without permission. Android ID: A-31081987. **Reference: CVE-2016-6709**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/155
Bypass	25/11/2016	2.1	An elevation of privilege in the System UI in Android 7.0 before 2016-11-01 could enable a local malicious user to bypass the security prompt of your work profile in Multi-Window mode. This issue is rated as High because it is a local bypass of user interaction requirements for any developer or security setting modifications. Android ID: A-30693465. **Reference: CVE-2016-6708**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/156

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; Gain Privileges	25/11/2016	9.3	An elevation of privilege vulnerability in System Server in Android 6.x before 2016-11-01 and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-31350622. **Reference: CVE-2016-6707**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/157
Execute Code; Gain Privileges	25/11/2016	9.3	An elevation of privilege vulnerability in Mediaserver in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-30907212. **Reference: CVE-2016-6705**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/158
Execute Code; Gain Privileges	25/11/2016	9.3	An elevation of privilege vulnerability in Mediaserver in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, 6.x before 2016-11-01, and 7.0 before 2016-11-01 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/159

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

			to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Android ID: A-30229821. **Reference: CVE-2016-6704**		
Execute Code	25/11/2016	6.8	A remote code execution vulnerability in an Android runtime library in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-11-01 could enable an attacker using a specially crafted payload to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses the Android runtime. Android ID: A-30765246. **Reference: CVE-2016-6703**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/160
Execute Code	25/11/2016	6.8	A remote code execution vulnerability in libjpeg in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses libjpeg. Android ID: A-30259087. **Reference: CVE-2016-6702**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/161
Execute Code; Overflow; Memory Corruption	25/11/2016	6.8	A remote code execution vulnerability in libskia in Android 7.0 before 2016-11-01 could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/162

			as High due to the possibility of remote code execution within the context of the gallery process. Android ID: A-30190637. **Reference: CVE-2016-6701**		
Execute Code	25/11/2016	9.3	An elevation of privilege vulnerability in libzipfile in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30916186. **Reference: CVE-2016-6700**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/163
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30741851. References: Qualcomm QC-CR#1058826. **Reference: CVE-2016-6698**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/164
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver,	https://source.android.com/security/bulletin/2016-11-	O-GOO-ANDRO--71216/165

			and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30593266. References: Qualcomm QC-CR#1054352. **Reference: CVE-2016-3907**	01.html	
Gain Information	25/11/2016	4.3	An information disclosure vulnerability in Qualcomm components including the GPU driver, power driver, SMSM Point-to-Point driver, and sound driver in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30445973. References: Qualcomm QC-CR#1054344. **Reference: CVE-2016-3906**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/166
Execute Code	25/11/2016	6.8	An elevation of privilege vulnerability in the Qualcomm bus driver in Android before 2016-11-05 could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Android ID: A-30311977. References: Qualcomm QC-CR#1050455. **Reference: CVE-2016-3904**	https://source.android.com/security/bulletin/2016-11-01.html	O-GOO-ANDRO--71216/167
Linux					
Linux Kernel The Linux kernel is a monolithic Unix-like computer operating system kernel.					

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; Gain Information	16/11/2016	4.3	The nfnetlink_rcv_batch function in net/netfilter/nfnetlink.c in the Linux kernel before 4.5 does not check whether a batch message's length field is large enough, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (infinite loop or out-of-bounds read) by leveraging the CAP_NET_ADMIN capability. **Reference: CVE-2016-7917**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=c58d6c93680f28ac58984af61d0a7ebf4319c241	O-LIN-LINUX--71216/168
Gain Information	16/11/2016	4.7	Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/*/environ file during a process-setup time interval in which environment-variable copying is incomplete. **Reference: CVE-2016-7916**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.5.4	O-LIN-LINUX--71216/169
Denial of Service; Gain Information	16/11/2016	4.3	The hid_input_field function in drivers/hid/hid-core.c in the Linux kernel before 4.6 allows physically proximate attackers to obtain sensitive information from kernel memory or cause a denial of service (out-of-bounds read) by connecting a device, as demonstrated by a Logitech DJ receiver. **Reference: CVE-2016-7915**	https://github.com/torvalds/linux/commit/50220dead1650609206efe91f0cc116132d59b3f	O-LIN-LINUX--71216/170
Denial of Service; Gain Information	16/11/2016	7.1	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.5.3 does not check whether a slot is a leaf,	https://github.com/torvalds/linux/commit/8d4a2ec1e0b41b0cf9a0c5cd4	O-LIN-LINUX--71216/171

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

			which allows local users to obtain sensitive information from kernel memory or cause a denial of service (invalid pointer dereference and out-of-bounds read) via an application that uses associative-array data structures, as demonstrated by the keyutils test suite. **Reference: CVE-2016-7914**	511da7f8e4f3de2	
Denial of Service; Gain Privileges	16/11/2016	9.3	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure. **Reference: CVE-2016-7913**	https://github.com/torvalds/linux/commit/8dfbcc4351a0b6d2f2d77f367552f48ffefafe18	O-LIN-LINUX--71216/172
Gain Privileges	16/11/2016	9.3	Use-after-free vulnerability in the ffs_user_copy_worker function in drivers/usb/gadget/function/f_fs.c in the Linux kernel before 4.5.3 allows local users to gain privileges by accessing an I/O data structure after a certain callback call. **Reference: CVE-2016-7912**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=38740a5b87d53ceb89eb2c970150f6e94e00373a	O-LIN-LINUX--71216/173
Denial of Service; Gain Privileges	16/11/2016	9.3	Race condition in the get_task_ioprio function in block/ioprio.c in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted ioprio_get system call. **Reference: CVE-2016-7911**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.6.6	O-LIN-LINUX--71216/174
Gain Privileges	16/11/2016	9.3	Use-after-free vulnerability in the disk_seqf_stop function in	http://git.kernel.org/cgit	O-LIN-LINUX--

			block/genhd.c in the Linux kernel before 4.7.1 allows local users to gain privileges by leveraging the execution of a certain stop operation even if the corresponding start operation had failed. **Reference: CVE-2016-7910**	/linux/kernel/git/torvalds/linux.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84	71216/175
Gain Information	16/11/2016	7.1	The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure. **Reference: CVE-2015-8964**	https://github.com/torvalds/linux/commit/dd42bf1197144ede075a9d4793123f7689e164bc	O-LIN-LINUX--71216/176
Denial of Service; Gain Privileges	16/11/2016	7.6	Race condition in kernel/events/core.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect handling of an swevent data structure during a CPU unplug operation. **Reference: CVE-2015-8963**	https://github.com/torvalds/linux/commit/12ca6ad2e3a896256f086497a7c7406a547ee373	O-LIN-LINUX--71216/177
Denial of Service; Gain Privileges; Memory Corruption	16/11/2016	9.3	Double free vulnerability in the sg_common_write function in drivers/scsi/sg.c in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (memory corruption and system crash) by detaching a device during an SG_IO ioctl call. **Reference: CVE-2015-8962**	https://source.android.com/security/bulletin/2016-11-01.html	O-LIN-LINUX--71216/178
Denial of Service; Gain Privileges	16/11/2016	9.3	The __ext4_journal_stop function in fs/ext4/ext4_jbd2.c in the Linux kernel before 4.3.3 allows local users to gain privileges or cause a denial of	https://source.android.com/security/bulletin/2016-11-01.html	O-LIN-LINUX--71216/179

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

			service (use-after-free) by leveraging improper access to a certain error field. **Reference: CVE-2015-8961**		
NA	27/11/2016	9.3	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel 4.4.22 through 4.4.28 contains extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a crafted application. NOTE: this vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels. **Reference: CVE-2016-9644**	https://lwn.net/Articles/705220/	O-LIN-LINUX--71216/180
Denial of Service	27/11/2016	10	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data. **Reference: CVE-2016-9555**	https://github.com/torvalds/linux/commit/bf911e985d6bbaa328c20c3e05f4eb03de11fdd6	O-LIN-LINUX--71216/181
Denial of Service	27/11/2016	9.3	security/keys/big_key.c in the Linux kernel before 4.8.7 mishandles unsuccessful crypto registration in conjunction with successful key-type registration, which allows local users to cause a denial of service (NULL pointer dereference and panic) or possibly have unspecified other impact via a crafted application that uses	https://github.com/torvalds/linux/commit/7df3e59c3d1df4f87fe874c7956ef7a3d2f4d5fb	O-LIN-LINUX--71216/182

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

			the big_key data type. **Reference: CVE-2016-9313**		
Denial of Service	27/11/2016	4.9	The cgroup offline implementation in the Linux kernel through 4.8.11 mishandles certain drain operations, which allows local users to cause a denial of service (system hang) by leveraging access to a container environment for executing a crafted application, as demonstrated by trinity. **Reference: CVE-2016-9191**	https://bugzilla.redhat.com/show_bug.cgi?id=1392439	O-LIN-LINUX--71216/183
Gain Information	27/11/2016	2.1	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel before 4.7.5 does not initialize a certain integer variable, which allows local users to obtain sensitive information from kernel stack memory by triggering failure of a get_user_ex call. **Reference: CVE-2016-9178**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=1c109fabbd51863475cd12ac206bdd249aee35af	O-LIN-LINUX--71216/184
Denial of Service; Overflow	27/11/2016	4.6	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file. **Reference: CVE-2016-9084**	https://patchwork.kernel.org/patch/9373631/	O-LIN-LINUX--71216/185
Denial of Service; Overflow; Memory Corruption; Bypass	27/11/2016	7.2	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access	https://patchwork.kernel.org/patch/9373631/	O-LIN-LINUX--71216/186

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

			to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug." **Reference: CVE-2016-9083**		
Denial of Service; Memory Corruption	27/11/2016	4.9	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent. **Reference: CVE-2016-8650**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=f5527fffff3f002b0a6b376163613b82f69de073	O-LIN-LINUX--71216/187
Denial of Service	27/11/2016	4.9	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a denial of service (OOPS) by attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data. **Reference: CVE-2016-8646**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4afa5f9617927453ac04b24b584f6c718dfb4f45	O-LIN-LINUX--71216/188
Denial of Service	27/11/2016	4.9	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c. **Reference: CVE-2016-8645**	https://bugzilla.redhat.com/show_bug.cgi?id=1393904	O-LIN-LINUX--71216/189
Execute Code; Overflow	27/11/2016	6.2	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remote attackers to execute arbitrary code via crafted fragmented packets.	https://bugzilla.redhat.com/show_bug.cgi?id=1391490	O-LIN-LINUX--71216/190

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-2016-8633		
Denial of Service; Overflow; Gain Privileges	27/11/2016	7.2	The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) by leveraging the CAP_NET_ADMIN capability. **Reference: CVE-2016-8632**	https://bugzilla.redhat.com/show_bug.cgi?id=1390832	O-LIN-LINUX--71216/191
Denial of Service	27/11/2016	4.9	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows local users to cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction. **Reference: CVE-2016-8630**	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=d9092f52d7e61dd1557f2db2400ddb430e85937e	O-LIN-LINUX--71216/192
Denial of Service	27/11/2016	4.9	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been performed on an AF_ALG socket before an accept system call is processed, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c. **Reference: CVE-2015-8970**	https://groups.google.com/forum/#%21msg/syzkaller/frb2XrB5aWk/xCXzkIBcDAAJ	O-LIN-LINUX--71216/193
Paloaltonetworks					
Pan-os Panos is a discontinued computer operating system developed by Acorn Computers in the 1980s, which ran on the 32016 Second Processor for the BBC Micro and the Acorn Cambridge Workstation.					

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

Gain Privileges	19/11/2016	4.6	Palo Alto Networks PAN-OS before 5.0.20, 5.1.x before 5.1.13, 6.0.x before 6.0.15, 6.1.x before 6.1.15, 7.0.x before 7.0.11, and 7.1.x before 7.1.6 allows local users to gain privileges via crafted values of unspecified environment variables. **Reference: CVE-2016-9151**	https://securityadvisories.paloaltonetworks.com/Home/Detail/67	O-PAL-PAN-O--71216/194
Execute Code; Overflow	19/11/2016	10	Buffer overflow in the management web interface in Palo Alto Networks PAN-OS before 5.0.20, 5.1.x before 5.1.13, 6.0.x before 6.0.15, 6.1.x before 6.1.15, 7.0.x before 7.0.11, and 7.1.x before 7.1.6 allows remote attackers to execute arbitrary code via unspecified vectors. **Reference: CVE-2016-9150**	https://securityadvisories.paloaltonetworks.com/Home/Detail/68	O-PAL-PAN-O--71216/195
NA	19/11/2016	4	The Addresses Object parser in Palo Alto Networks PAN-OS before 5.0.20, 5.1.x before 5.1.13, 6.0.x before 6.0.15, 6.1.x before 6.1.15, 7.0.x before 7.0.11, and 7.1.x before 7.1.6 mishandles single quote characters, which allows remote authenticated users to conduct XPath injection attacks via a crafted string. **Reference: CVE-2016-9149**	https://securityadvisories.paloaltonetworks.com/Home/Detail/70	O-PAL-PAN-O--71216/196
Samsung					
Samsung Mobile Samsung is the largest mobile phone maker in its home market of South Korea, and the third largest in the world. In addition to mobile phones and related devices, the company also manufacturers things such as televisions, cameras, and electronic components.					
Gain Information	23/11/2016	4.3	The mDNIe system service on Samsung Mobile S7 devices with M(6.0) software does not properly restrict setmDNIeScreenCurtain API calls, enabling attackers to control a device's screen. This	http://security.samsungmobile.com/smrupdate.html#SMR-NOV-2016	O-SAM-SAMSU--71216/197

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

			can be exploited via a crafted application to eavesdrop after phone shutdown or record a conversation. The Samsung ID is SVE-2016-6343. **Reference: CVE-2016-9567**		
Siemens					
Ccid1445-dn18 Firmware; Ccid1445-dn28 Firmware; Ccid1445-dn36 Firmware; Ccis1425 Firmware; Ccmd3025-dn18 Firmware; Ccms2025 Firmware; Ccmw1025 Firmware; Ccmw3025 Firmware; Ccpw3025 Firmware; Cfis1425 Firmware; Cfms2025 Firmware; Cfmw1025 Firmware; Cfmw3025 Firmware; Cvms2025-ir Firmware; Cvmw3025-ir Firmware NA					
NA	22/11/2016	5	The following SIEMENS branded IP Camera Models CCMW3025, CVMW3025-IR, CFMW3025 prior to version 1.41_SP18_S1; CCPW3025, CCPW5025 prior to version 0.1.73_S1; CCMD3025-DN18 prior to version v1.394_S1; CCID1445-DN18, CCID1445-DN28, CCID1145-DN36, CFIS1425, CCIS1425, CFMS2025, CCMS2025, CVMS2025-IR, CFMW1025, CCMW1025 prior to version v2635_SP1 could allow an attacker with network access to the web server to obtain administrative credentials under certain circumstances. **Reference: CVE-2016-9155**	https://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-284765.pdf	O-SIE-CCID1--71216/198
Simatic Cp 1543-1 Firmware NA					
Denial of Service	18/11/2016	3.5	Siemens SIMATIC CP 1543-1 before 2.0.28, when SNMPv3 write access or SNMPv1 is enabled, allows remote authenticated users to cause a denial of service by modifying SNMP variables. **Reference: CVE-2016-8562**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-672373.pdf	O-SIE-SIMAT--71216/199
Gain Privileges	18/11/2016	6	Siemens SIMATIC CP 1543-1 before 2.0.28 allows remote authenticated users to gain	http://www.siemens.com/cert/pool	O-SIE-SIMAT--71216/

			privileges by leveraging certain TIA-Portal access and project-data access. **Reference: CVE-2016-8561**	/cert/siemens_security_advisory_ssa-672373.pdf	200
Simatic Cp 343-1 Firmware; Simatic Cp 443-1 Firmware; Simatic S7 300 Cpu Firmware; Simatic S7 400 Cpu Firmware NA					
Cross Site Request Forgery	23/11/2016	6.8	Cross-site request forgery (CSRF) vulnerability in the integrated web server on Siemens SIMATIC CP 343-1 Advanced before 3.0.53, SIMATIC CP 443-1 Advanced, SIMATIC S7-300 CPU, and SIMATIC S7-400 CPU devices allows remote attackers to hijack the authentication of arbitrary users. **Reference: CVE-2016-8673**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-603476.pdf	O-SIE-SIMAT--71216/201
Gain Information	23/11/2016	5	The integrated web server on Siemens SIMATIC CP 343-1 Advanced before 3.0.53, SIMATIC CP 443-1 Advanced, SIMATIC S7-300 CPU, and SIMATIC S7-400 CPU devices does not set the secure flag for unspecified cookies in an https session, which makes it easier for remote attackers to capture these cookies by intercepting their transmission within an http session. **Reference: CVE-2016-8672**	http://www.siemens.com/cert/pool/cert/siemens_security_advisory_ssa-603476.pdf	O-SIE-SIMAT--71216/202