National Critical Information Infrastructure Protection Centre

CVE Report

16-31 August 2017 **Vol. 04 No.14**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Accellion					
Sametime					
XSS	18-08-2017	7.5	IBM Sametime 8.5.2 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 113935. **CVE-2016-2975**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-ACC-SAMET-140817/1
Alcatel-lucent					
Emptoris Strategic Supply Management					
XSS	18-08-2017	7.5	IBM Emptoris Strategic Supply Management Platform 10.0 and 10.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 116755. **CVE-2016-6021**	http://www.ibm.com/support/docview.wss?uid=swg22006799	A-ALC-EMPTO-140817/2
Apache					
Android					
+Info	17-08-2017	6.8	A information disclosure vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37712181. **CVE-2017-0739**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/3
Android					
NA	17-08-2017	6.8	A information disclosure vulnerability in the Android	https://source.android.c	A-APA-ANDRO-

			media framework (audioserver). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37563371. **CVE-2017-0738**	om/security/bulletin/2017-08-01	140817/4
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37563942. **CVE-2017-0737**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/5
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37504237. **CVE-2017-0732**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/6
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework (mpeg4 encoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36075363. **CVE-2017-0731**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/7
DoS	17-08-2017	6.8	A denial of service vulnerability in the Android media framework (h264 decoder). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36279112. **CVE-2017-0730**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/8
NA	18-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework (mediadrmserver). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37710346. **CVE-2017-0729**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/9
DoS	18-08-2017	6.8	A denial of service vulnerability in the Android media framework	https://source.android.c	A-APA-ANDRO-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			(hevc decoder). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37469795. **CVE-2017-0728**	om/security/bulletin/2017-08-01	140817/10
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37430213. **CVE-2017-0720**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/11
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (mpeg2 decoder). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37273673. **CVE-2017-0719**	https://source.android.com/security/bulletin/2017-08-01	A-APA-ANDRO-140817/12
NA	18-08-2017	6.9	In all Qualcomm products with Android releases from CAF using the Linux kernel, when downloading a file, an excessive amount of memory may be consumed. **CVE-2016-10390**	https://source.android.com/security/bulletin/2017-07-01	A-APA-ANDRO-140817/13
NTP					
DoS Exec Code Overflow	24-08-2017	7.6	Buffer overflow in the password management functionality in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted key file. **CVE-2015-7854**	https://bugzilla.redhat.com/show_bug.cgi?id=1274263	A-APA-NTP-140817/14
DoS Exec Code Overflow	24-08-2017	7.6	The datalen parameter in the refclock driver in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to execute arbitrary code or cause a denial of service (crash) via a negative input value. **CVE-2015-7853**	https://bugzilla.redhat.com/show_bug.cgi?id=1274262	A-APA-NTP-140817/15
DoS Exec Code	24-08-2017	7.6	Use-after-free vulnerability in ntpd in NTP 4.2.x before 4.2.8p4,	https://bugzilla.redhat.c	A-APA-NTP-140817/16

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			and 4.3.x before 4.3.77 allows remote authenticated users to possibly execute arbitrary code or cause a denial of service (crash) via crafted packets. **CVE-2015-7849**	om/show_bug.cgi?id=1274257	
NA	24-08-2017	7.6	The rate limiting feature in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to have unspecified impact via a large number of crafted requests. **CVE-2015-7705**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05270839	A-APA-NTP-140817/17
Lemur					
NA	24-08-2017	7.6	Lemur 0.1.4 does not use sufficient entropy in its IV when encrypting AES in CBC mode. **CVE-2015-7764**	https://github.com/Netflix/lemur/issues/117	A-APA-LEMUR-140817/18
Artifex					
Android					
DoS	17-08-2017	6.8	A denial of service vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-38487564. **CVE-2017-0736**	https://source.android.com/security/bulletin/2017-08-01	A-ART-ANDRO-140817/19
Arubanetworks					
Android					
+Info	18-08-2017	7.5	In an ioctl handler in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, if a user supplies a value too large, then an out-of-bounds read occurs. **CVE-2016-5858**	https://source.android.com/security/bulletin/2017-05-01	A-ARU-ANDRO-140817/20
Tomcat					
Bypass	18-08-2017	7.5	In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications.	NA	A-ARU-TOMCA-140817/21

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE-2016-5018		
Pony Mail					
Bypass	18-08-2017	7.5	Apache Pony Mail 0.6c through 0.8b allows remote attackers to bypass authentication. **CVE-2016-4460**	http://markmail.org/message/jy7o23cppny26icu	A-ARU-PONY -140817/22
Gnutls					
NA	18-08-2017	7.5	The "GNUTLS_KEYLOGFILE" environment variable in gnutls 3.4.12 allows remote attackers to overwrite and corrupt arbitrary files in the filesystem. **CVE-2016-4456**	https://bugzilla.redhat.com/show_bug.cgi?id=1343505	A-ARU-GNUTL-140817/23
Ovirt					
XSS	18-08-2017	7.5	Cross-site scripting (XSS) vulnerability in ovirt-engine allows remote attackers to inject arbitrary web script or HTML. **CVE-2016-3113**	https://bugzilla.redhat.com/show_bug.cgi?id=1326598	A-ARU-OVIRT-140817/24
Sametime					
NA	18-08-2017	7.5	The Sametime WebPlayer 8.5.2 and 9.0 is vulnerable to a script injection where a malicious site can inject their own script by exploiting a vulnerability in the way that the WebPlayer works. IBM X-Force ID: 113993. **CVE-2016-2980**	http://www.ibm.com/support/docview.wss?uid=swg22006447	A-ARU-SAMET-140817/25
Attic Project					
Mrd-305-din Firmware;Mrd-315-din Firmware;Mrd-355-din Firmware;Mrd-455-din Firmware					
NA	18-08-2017	7.5	A Use of Hard-Coded Cryptographic Key issue was discovered in MRD-305-DIN versions older than 1.7.5.0, and MRD-315, MRD-355, MRD-455 versions older than 1.7.5.0. The device utilizes hard-coded private cryptographic keys that may allow an attacker to decrypt traffic from any other source. **CVE-2016-5816**	https://ics-cert.us-cert.gov/advisories/ICSA-17-236-01	A-ATT-MRD-3-140817/26
Barracuda					
Android					
NA	22-08-2017	7.5	In all Qualcomm products with Android releases from CAF using	https://source.android.	A-BAR-ANDRO-

			the Linux kernel, a vulnerability exists in eMBMS where an assertion can be reached by a sequence of downlink messages. **CVE-2015-9039**	com/security/bulletin/2017-07-01	140817/27
NA	22-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a NULL pointer may be dereferenced in the front end. **CVE-2015-9038**	https://source.android.com/security/bulletin/2017-07-01	A-BAR-ANDRO-140817/28
BMC					
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in the processing of lost RTP packets.**CVE-2015-9048**	https://source.android.com/security/bulletin/2017-07-01	A-BMC-ANDRO-140817/29
Broken Link Checker Project					
Android					
Overflow	18-08-2017	7.5	In an audio driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, if a function is called with a very large length, an integer overflow could occur followed by a heap buffer overflow. **CVE-2016-5860**	https://source.android.com/security/bulletin/2017-05-01	A-BRO-ANDRO-140817/30
Busybox					
NTP					
DoS	24-08-2017	7.6	ntpq in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted mode 6 response packets. **CVE-2015-7852**	http://support.ntp.org/bin/view/Main/NtpBug2919	A-BUS-NTP-140817/31
Capnproto					
Sametime					
NA	18-08-2017	7.5	IBM Sametime 8.5.1 and 9.0 could allow an authenticated user to enumerate meeting rooms by guessing the meeting room id. IBM X-Force ID: 113847. **CVE-2016-2966**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-CAP-SAMET-140817/33
CSRF	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 is vulnerable to	http://www.ibm.com/	A-CAP-SAMET-140817/34

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			cross-site request forgery, caused by improper validation of user-supplied input. By persuading a user to visit a malicious link, a remote attacker could force the user to log out of Sametime. IBM X-Force ID: 113846. **CVE-2016-2965**	support/docview.wss?uid=swg22006439	
NA	18-08-2017	7.5	IBM Sametime 8.5.2 and 9.0 under certain conditions provides an error message to a user that is too detailed and may reveal details about the application. IBM X-Force ID: 113813.**CVE-2016-2964**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-CAP-SAMET-140817/35
NA	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 could allow a meeting room manager to remove the primary managers privileges. IBM X-Force ID: 113804.**CVE-2016-2959**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-CAP-SAMET-140817/36
Chaos Tool Suite Project					
Android					
Overflow	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, sSL handshake failure with ClientHello rejection results in memory leak. **CVE-2016-10343**	https://source.android.com/security/bulletin/2017-07-01	A-CHA-ANDRO-140817/37
Cisco					
NTP					
DoS Overflow	24-08-2017	7.6	ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote authenticated users to cause a denial of service (infinite loop or crash) by pointing the key file at the log file. **CVE-2015-7850**	https://bugzilla.redhat.com/show_bug.cgi?id=1274258	A-CIS-NTP-140817/38
Cloud4wi					
Android					
Overflow	18-08-2017	7.5	In a sound driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, if a function is called with a very large length, an integer overflow	https://source.android.com/security/bulletin/2017-05-01	A-CLO-ANDRO-140817/39

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			could occur followed by a buffer overflow. **CVE-2016-5859**		
Coremail					
Trend Micro Control Manager					
+Info	18-08-2017	7.2	Information Disclosure vulnerability in the Dashboard and Error Pages in Trend Micro Control Manager SP3 6.0. **CVE-2016-6220**	https://success.trendmicro.com/solution/1114749	A-COR-TREND-140817/40
Digium					
Sametime					
NA	18-08-2017	7.5	IBM Sametime Connect 8.5.2 and 9.0, after uninstalling the Sametime Rich Client, could disclose potentially sensitive information related to the Sametime environment as well as other users on the local machine of the user. IBM X-Force ID: 113934.**CVE-2016-2974**	http://www.ibm.com/support/docview.wss?uid=swg22006444	A-DIG-SAMET-140817/41
Django-cms					
Android					
NA	18-08-2017	7.5	When a control related to codec is issued from userspace in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, the type casting is done to the container structure instead of the codec's individual structure, resulting in a device restart after kernel crash occurs.**CVE-2016-5862**	https://source.android.com/security/bulletin/2017-05-01	A-DJA-ANDRO-140817/42
Downloadmanager					
Android					
Overflow	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists when processing a QMI message. **CVE-2015-9042**	https://source.android.com/security/bulletin/2017-07-01	A-DOW-ANDRO-140817/43
Elasticsearch					
Android					
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an integer	https://source.android.com/securit	A-ELA-ANDRO-140817/44

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			overflow to buffer overflow vulnerability exists when loading an image file.**CVE-2016-5871**	y/bulletin/ 2017-07-01	
Exec Code	18-08-2017	7.5	In an audio driver in all Qualcomm products with Android releases from CAF using the Linux kernel, when a sanity check encounters a length value not in the correct range, an error message is printed, but code execution continues in the same way as for a correct length value. **CVE-2016-5853**	https://source.android.com/security/bulletin/2017-05-01	A-ELA-ANDRO-140817/45
Exponentcms					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an untrusted pointer dereference can occur in a TrustZone syscall. **CVE-2015-9072**	https://source.android.com/security/bulletin/2017-07-01	A-EXP-ANDRO-140817/46
Expressjs					
Android					
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, an incorrect length is used to clear a memory buffer resulting in adjacent memory getting corrupted. **CVE-2015-9036**	https://source.android.com/security/bulletin/2017-07-01	A-EXP-ANDRO-140817/47
Ffmpeg					
Ganeti					
DoS	24-08-2017	7.6	The RESTful control interface (aka RAPI or ganeti-rapi) in Ganeti before 2.9.7, 2.10.x before 2.10.8, 2.11.x before 2.11.8, 2.12.x before 2.12.6, 2.13.x before 2.13.3, 2.14.x before 2.14.2, and 2.15.x before 2.15.2, when used in SSL mode, allows remote attackers to cause a denial of service (resource consumption) via SSL parameter renegotiation.**CVE-2015-7944**	http://docs.ganeti.org/ganeti/2.13/html/news.html#version-2-13-3	A-FFM-GANET-140817/48
Galaxy S6 Edge Firmware					
DoS Exec	24-08-2017	7.6	The DCMProvider service in	NA	A-FFM-GALAX-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Code Overflow			Samsung LibQjpeg on a Samsung SM-G925V device running build number LRX22G.G925VVRU1AOE2 allows remote attackers to cause a denial of service (segmentation fault and process crash) and execute arbitrary code via a crafted JPG.**CVE-2015-7894**		140817/49
Samsung Mobile					
NA	24-08-2017	7.6	Race condition in the ioctl implementation in the Samsung Graphics 2D driver (aka /dev/fimg2d) in Samsung devices with Android L(5.0/5.1) allows local users to trigger memory errors by leveraging definition of g2d_lock and g2d_unlock lock macros as no-ops, aka SVE-2015-4598. **CVE-2015-7891**	http://security.samsungmobile.com/smrupdate.html#SMR-OCT-2015	A-FFM-SAMSU-140817/50
Snapcenter Server					
NA	24-08-2017	7.6	NetApp SnapCenter Server 1.0 allows remote authenticated users to list and delete backups. **CVE-2015-7887**	https://kb.netapp.com/support/s/article/ka51A00000007EnQAI/authentication-bypass-vulnerability-in-snapcenter-server-1-0?language=en_US	A-FFM-SNAPC-140817/51
Ctools					
NA	24-08-2017	7.6	ctools 6.x-1.x before 6.x-1.14 and 7.x-1.x before 7.x-1.8 in Drupal does not verify the "edit" permission for the "content type" plugins that are used on Panels and similar systems to place content and functionality on a page.**CVE-2015-7875**	https://www.drupal.org/node/2554145	A-FFM-CTOOL-140817/52
NTP					
Bypass	24-08-2017	7.6	Crypto-NAK packets in ntpd in	https://bug	A-FFM-NTP-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.**CVE-2015-7871**	zilla.redhat.com/show_bug.cgi?id=1274265	140817/53
DoS	24-08-2017	7.6	The decodenetnum function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (assertion failure) via a 6 or mode 7 packet containing a long data value. **CVE-2015-7855**	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05270839	A-FFM-NTP-140817/54
F-secure					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, the UE can send unprotected MeasurementReports revealing UE location.**CVE-2016-10380**	https://source.android.com/security/bulletin/2017-07-01	A-F-S-ANDRO-140817/55
Ganeti Project					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, an argument to a hypervisor function is not properly validated. **CVE-2016-10347**	https://source.android.com/security/bulletin/2017-07-01	A-GAN-ANDRO-140817/56
Overflow	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, an integer overflow vulnerability exists in the hypervisor. **CVE-2016-10346**	https://source.android.com/security/bulletin/2017-07-01	A-GAN-ANDRO-140817/57
Gigaccsecure					
Android					
DoS	17-08-2017	6.8	A denial of service vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-38239864. **CVE-2017-0735**	https://source.android.com/security/bulletin/2017-08-01	A-GIG-ANDRO-140817/58
DoS	17-08-2017	6.8	A denial of service vulnerability in the Android media framework (libavc). Product: Android.	https://source.android.com/securit	A-GIG-ANDRO-140817/59

			Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-38014992. **CVE-2017-0734**	y/bulletin/ 2017-08-01	
Gnome					
Sametime					
NA	18-08-2017	7.5	IBM Sametime 8.5 and 9.0 meetings server may provide detailed information in an error message that may provide details about the application to possible attackers. IBM X-Force ID: 113851.**CVE-2016-2970**	http://www.ibm.com/support/docview.wss?uid=swg22006233	A-GNO-SAMET-140817/60
GNU					
Android					
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in LTE where an assertion can be reached due to an improper bound on the size of a frequency list.**CVE-2015-9046**	https://source.android.com/security/bulletin/2017-07-01	A-GNU-ANDRO-140817/61
Gnutls					
Android					
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (mpeg2 decoder). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37273547. **CVE-2017-0718**	https://source.android.com/security/bulletin/2017-08-01	A-GNU-ANDRO-140817/62
Good					
Android					
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a string can fail to be null-terminated in SIP leading to a buffer overflow. **CVE-2015-9034**	https://source.android.com/security/bulletin/2017-07-01	A-GOO-ANDRO-140817/63
Google;Redhat					
Jboss Enterprise Application Platform					
+Info	18-08-2017	7.2	Get requests in JBoss Enterprise Application Platform (EAP) 7 disclose internal IP addresses to remote attackers. **CVE-2016-6311**	https://bugzilla.redhat.com/show_bug.cgi?id=1362735	A-GOO-JBOSS-140817/64
Graphviz					

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

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Android					
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, validation of buffer lengths is missing in malware protection. **CVE-2015-8596**	https://source.android.com/security/bulletin/2017-07-01	A-GRA-ANDRO-140817/65
Grml					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an untrusted pointer dereference can occur in a TrustZone syscall. **CVE-2015-9073**	https://source.android.com/security/bulletin/2017-07-01	A-GRM-ANDRO-140817/66
Haproxy					
Android					
NA	18-08-2017	6.8	In all Qualcomm products with Android releases from CAF using the Linux kernel, the length in an HCI command is not properly checked for validity. **CVE-2016-10391**	https://source.android.com/security/bulletin/2017-07-01	A-HAP-ANDRO-140817/67
Helpdesk Pro Project					
Puppet Enterprise					
Exec Code	18-08-2017	7.5	The console in Puppet Enterprise 2015.x and 2016.x prior to 2016.4.0 includes unsafe string reads that potentially allows for remote code execution on the console node. **CVE-2016-5716**	https://puppet.com/security/cve/pe-console-oct-2016	A-HEL-PUPPE-140817/68
HP					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, the Secure File System can become corrupted. **CVE-2015-9069**	https://source.android.com/security/bulletin/2017-07-01	A-HP-ANDRO-140817/69
IBM					
Emptoris Sourcing					
XSS	16-08-2017	6.8	IBM Emptoris Sourcing 9.5 - 10.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI	http://www-01.ibm.com/support/docview.wss?	A-IBM-EMPTO-140817/70

			thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128172.**CVE-2017-1447**	uid=swg22005834	
Emptoris Spend Analysis					
XSS	16-08-2017	6.8	IBM Emptoris Spend Analysis 9.5.0.0 through 10.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128171. **CVE-2017-1446**	http://www-01.ibm.com/support/docview.wss?uid=swg22005787	A-IBM-EMPTO-140817/71
XSS	16-08-2017	6.8	IBM Emptoris Spend Analysis 9.5.0.0 through 10.1.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128170. **CVE-2017-1445**	http://www-01.ibm.com/support/docview.wss?uid=swg22005787	A-IBM-EMPTO-140817/80
Emptoris Sourcing					
XSS	16-08-2017	6.8	IBM Emptoris Sourcing 9.5 - 10.1.3 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128110.**CVE-2017-1444**	http://www-01.ibm.com/support/docview.wss?uid=swg22005834	A-IBM-EMPTO-140817/81
Emptoris Services Procurement					
XSS	16-08-2017	6.8	IBM Emptoris Services Procurement 10.0.0.5 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality	http://www-01.ibm.com/support/docview.wss?uid=swg22005550	A-IBM-EMPTO-140817/82

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 128109. **CVE-2017-1443**		
Emptoris Services Procurement					
CSRF	16-08-2017	6.8	IBM Emptoris Services Procurement 10.0.0.5 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 128107.**CVE-2017-1442**	http://www-01.ibm.com/support/docview.wss?uid=swg22005550	A-IBM-EMPTO-140817/83
NA	16-08-2017	6.8	IBM Emptoris Services Procurement 10.0.0.5 could allow a local user to view sensitive information stored locally due to improper access control. IBM X-Force ID: 128106. **CVE-2017-1441**	http://www-01.ibm.com/support/docview.wss?uid=swg22005550	A-IBM-EMPTO-140817/84
Exec Code	16-08-2017	6.8	IBM Emptoris Services Procurement 10.0.0.5 could allow a remote attacker to include arbitrary files. A remote attacker could send a specially-crafted URL to specify a malicious file from a remote system, which could allow the attacker to execute arbitrary code on the vulnerable Web server. IBM X-Force ID: 128105. **CVE-2017-1440**	http://www-01.ibm.com/support/docview.wss?uid=swg22005550	A-IBM-EMPTO-140817/85
Infosphere Streams					
XSS	16-08-2017	6.8	IBM InfoSphere Streams 4.0, 4.1, and 4.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127632.**CVE-2017-1431**	http://www.ibm.com/support/docview.wss?uid=swg22006827	A-IBM-INFOS-140817/86
Cognos Analytics					
NA	16-08-2017	6.8	IBM Cognos Analytics 11.0 could allow a remote attacker to hijack	http://www.ibm.com/	A-IBM-COGNO-140817/87

			the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and possibly launch further attacks against the victim. IBM X-Force ID: 127583.**CVE-2017-1428**	support/docview.wss?uid=swg22007242	
XSS	16-08-2017	6.8	IBM Cognos Analytics 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127579. **CVE-2017-1427**	http://www.ibm.com/support/docview.wss?uid=swg22007242	A-IBM-COGNO-140817/88
Maas360 Dtm					
+Info	16-08-2017	6.8	IBM MaaS360 DTM all versions up to 3.81 does not perform proper verification for user rights of certain applications which could disclose sensitive information. IBM X-Force ID: 127412.**CVE-2017-1422**	http://www.ibm.com/support/docview.wss?uid=swg22006985	A-IBM-MAAS3-140817/89
Infosphere Information Server					
NA	16-08-2017	6.8	IBM InfoSphere Information Server 9.1, 11.3, and 11.5 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 127155. **CVE-2017-1383**	http://www.ibm.com/support/docview.wss?uid=swg22005803	A-IBM-INFOS-140817/90
Runbook Automation					
+Info	16-08-2017	6.8	IBM Runbook Automation reveals sensitive information in error messages that could be used in further attacks against the system. IBM X-Force ID: 126874.**CVE-2017-1377**	http://www.ibm.com/support/docview.wss?uid=swg22007031	A-IBM-RUNBO-140817/91
Maximo Asset Management;Maximo Asset Management Essentials					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	16-08-2017	6.8	IBM Maximo Asset Management 7.5 and 7.6 could allow an authenticated user to manipulate work orders to forge emails which could be used to conduct further advanced attacks. IBM X-Force ID: 126684. **CVE-2017-1357**	http://www.ibm.com/support/docview.wss?uid=swg22006647	A-IBM-MAXIM-140817/92
Rational Doors Next Generation;Rational Requirements Composer					
XSS	16-08-2017	6.8	IBM DOORS Next Generation (DNG/RRC) 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126246. **CVE-2017-1338**	http://www.ibm.com/support/docview.wss?uid=swg22004138	A-IBM-RATIO-140817/93
Content Navigator					
XSS	16-08-2017	6.8	IBM Content Navigator 2.0.3 and 3.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126233.**CVE-2017-1331**	http://www.ibm.com/support/docview.wss?uid=swg22003928	A-IBM-CONTE-140817/94
Inotes					
XSS	16-08-2017	6.8	IBM iNotes 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126062. **CVE-2017-1327**	http://www.ibm.com/support/docview.wss?uid=swg22003664	A-IBM-INOTE-140817/95
Infosphere Master Data Management Server					
XSS	17-08-2017	6.8	IBM InfoSphere Master Data Management Server 10.0, 11.0, 11.3, 11.4, 11.5, and 11.6 is vulnerable to cross-site scripting.	http://www.ibm.com/support/docview.wss?u	A-IBM-INFOS-140817/96

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 123674. **CVE-2017-1199**	id=swg22006618	
Curam Social Program Management					
+Info	17-08-2017	6.8	IBM Curam Social Program Management 6.0, 6.1, 6.2, and 7.0 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 123670. **CVE-2017-1195**	http://www.ibm.com/support/docview.wss?uid=swg22007160	A-IBM-CURAM-140817/97
Sterling B2b Integrator					
NA	17-08-2017	6.8	IBM Sterling B2B Integrator 5.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or consume memory resources. IBM X-Force ID: 123663. **CVE-2017-1192**	http://www.ibm.com/support/docview.wss?uid=swg22004267	A-IBM-STERL-140817/98
Emptoris Strategic Supply Management					
Exec Code	17-08-2017	6.8	IBM Emptoris Strategic Supply Management Platform 10.x and 10.1 could allow a local user with special access roles to execute arbitrary code on the system. By manipulating a configurable property, an attacker could exploit this vulnerability to gain	http://www.ibm.com/support/docview.wss?uid=swg22006799	A-IBM-EMPTO-140817/99

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			full control over the system. IBM X-Force ID: 123559. **CVE-2017-1190**		
Sterling B2b Integrator					
Sql	17-08-2017	6.8	IBM Sterling B2B Integrator Standard Edition 5.2 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 123296.**CVE-2017-1174**	http://www.ibm.com/support/docview.wss?uid=swg22004268	A-IBM-STERL-140817/100
Rational Engineering Lifecycle Manager					
XSS	17-08-2017	6.8	IBM Rational Engineering Lifecycle Manager 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 123187.**CVE-2017-1168**	http://www.ibm.com/support/docview.wss?uid=swg22006976	A-IBM-RATIO-140817/101
Websphere Mq Internet Pass-thru					
NA	17-08-2017	6.8	IBM WebSphere MQ Internet Pass-Thru 2.0 and 2.1 could allow n attacker to cause the MQIPT to stop responding due to an incorrectly configured security policy. IBM X-Force ID: 121156.**CVE-2017-1118**	http://www.ibm.com/support/docview.wss?uid=swg22006580	A-IBM-WEBSP-140817/102
Curam Social Program Management					
NA	17-08-2017	6.8	IBM Curam Social Program Management 6.0, 6.1, 6.2, and 7.0 contains an unspecified vulnerability that could allow an authenticated user to view the incidents of a higher privileged user. IBM X-Force ID: 120915. **CVE-2017-1110**	http://www.ibm.com/support/docview.wss?uid=swg22007161	A-IBM-CURAM-140817/103
Android					
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Qualcomm ipa driver. Product: Android.	https://source.android.com/securit	A-IBM-ANDRO-140817/104

			Versions: Android kernel. Android ID: A-35467471. References: QC-CR#2029392. **CVE-2017-0746**	y/bulletin/ 2017-08-01	
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the MediaTek video driver. Product: Android. Versions: Android kernel. Android ID: A-36074857. References: M-ALPS03275524. **CVE-2017-0742**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/105
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the MediaTek gpu driver. Product: Android. Versions: Android kernel. Android ID: A-32458601. References: M-ALPS03007523. **CVE-2017-0741**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/106
Exec Code	17-08-2017	6.8	A remote code execution vulnerability in the Broadcom networking driver. Product: Android. Versions: Android kernel. Android ID: A-37168488. References: B-RB#116402. **CVE-2017-0740**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/107
DoS	18-08-2017	6.8	A denial of service vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36819262. **CVE-2017-0724**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37968755.**CVE-2017-0723**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/108
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (h263 decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37660827.**CVE-2017-0722**	https://source.android.com/security/bulletin/ 2017-08-01	A-IBM-ANDRO-140817/109
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (libavc).	https://source.android.com/securit	A-IBM-ANDRO-140817/110

			Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36998372.**CVE-2017-0715**	y/bulletin/ 2017-08-01	
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (h263 decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36492637.**CVE-2017-0714**	https://source.android.com/security/bulletin/2017-08-01	A-IBM-ANDRO-140817/111
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android libraries (sfntly). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-32096780. **CVE-2017-0713**	https://source.android.com/security/bulletin/2017-08-01	A-IBM-ANDRO-140817/112
NA	18-08-2017	6.8	A elevation of privilege vulnerability in the Android framework (wi-fi service). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37207928. **CVE-2017-0712**	https://source.android.com/security/bulletin/2017-08-01	A-IBM-ANDRO-140817/113
DoS	18-08-2017	6.8	A denial of service vulnerability in the Android media framework (libavc). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35583675. **CVE-2017-0687**	https://source.android.com/security/bulletin/2017-08-01	A-IBM-ANDRO-140817/114
Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2008;Windows Server 2012;Windows Server 2016					
Exec Code Overflow	18-08-2017	6.8	Microsoft Windows PDF Library in Windows Server 2008 R2 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability when it improperly handles objects in memory, aka "Windows PDF Remote Code Execution Vulnerability".**CVE-2017-0293**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0293	A-IBM-WINDO-140817/115
Exec Code Overflow	18-08-2017	6.8	Microsoft JET Database Engine in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1,	https://portal.msrc.microsoft.com/e	A-IBM-WINDO-140817/116

			Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a remote code execution vulnerability due to buffer overflow, aka "Microsoft JET Database Engine Remote Code Execution Vulnerability". **CVE-2017-0250**	n-US/security-guidance/advisory/CVE-2017-0250	
DoS	18-08-2017	6.8	Windows NetBIOS in Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, Windows 10 Gold, 1511, 1607, 1703, and Windows Server 2016 allows a denial of service vulnerability when it improperly handles NetBIOS packets, aka "Windows NetBIOS Denial of Service Vulnerability".**CVE-2017-0174**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0174	A-IBM-WINDO-140817/117
Openjpeg					
DoS Overflow	18-08-2017	6.8	Integer overflow vulnerability in the bmp24toimage function in convertbmp.c in OpenJPEG before 2.2.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted bmp file.**CVE-2016-10507**	https://github.com/uclouvain/openjpeg/issues/833	A-IBM-OPENJ-140817/118
DoS	18-08-2017	6.8	Division-by-zero vulnerabilities in the functions opj_pi_next_cprl, opj_pi_next_pcrl, and opj_pi_next_rpcl in pi.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service (application crash) via crafted j2k files. **CVE-2016-10506**	https://github.com/uclouvain/openjpeg/commit/d27ccf01c68a31ad62b33d2dc1ba2bb1eeaafe7b	A-IBM-OPENJ-140817/119
DoS	18-08-2017	6.8	NULL pointer dereference vulnerabilities in the imagetopnm function in convert.c, sycc444_to_rgb function in color.c, color_esycc_to_rgb function in	https://github.com/uclouvain/openjpeg/issues/792	A-IBM-OPENJ-140817/120

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			color.c, and sycc422_to_rgb function in color.c in OpenJPEG before 2.2.0 allow remote attackers to cause a denial of service (application crash) via crafted j2k files. **CVE-2016-10505**		
DoS Overflow	18-08-2017	6.8	Heap-based buffer overflow vulnerability in the opj_mqc_byteout function in mqc.c in OpenJPEG before 2.2.0 allows remote attackers to cause a denial of service (application crash) via a crafted bmp file. **CVE-2016-10504**	https://github.com/uclouvain/openjpeg/issues/835	A-IBM-OPENJ-140817/121
Sametime					
NA	18-08-2017	6.8	IBM Sametime Meeting Server 8.5.2 and 9.0 could allow an authenticated and invited user of Sametime meeting to lower any or all hands in an e-meeting, thus spoofing results of votes in the meeting. IBM X-Force ID: 113803.**CVE-2016-10503**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-IBM-SAMET-140817/122
Liferay Portal					
XSS	18-08-2017	6.8	XSS exists in Liferay Portal before 7.0 CE GA4 via a crafted redirect field to modules/apps/foundation/frontend-js/frontend-js-spa-web/src/main/resources/META-INF/resources/init.jsp. **CVE-2016-10404**	https://dev.liferay.com/web/community-security-team/known-vulnerabilities/liferay-portal-70/-/asset_publisher/cjE0ourZXJZE/content/cst-7017-multiple-xss-vulnerabilities	A-IBM-LIFER-140817/123
Android					
Overflow	18-08-2017	6.8	In all Qualcomm products with Android releases from CAF using	https://source.android.	A-IBM-ANDRO-

			the Linux kernel, a driver can potentially leak kernel memory. **CVE-2016-10392**	com/security/bulletin/2017-07-01	140817/124
Overflow	18-08-2017	6.9	In all Qualcomm products with Android releases from CAF using the Linux kernel, there is no size check for the images being flashed onto the NAND memory in their respective partitions, so there is a possibility of writing beyond the intended partition. **CVE-2016-10389**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/125
NA	18-08-2017	6.9	In all Qualcomm products with Android releases from CAF using the Linux kernel, a configuration vulnerability exists when loading a 3rd-party QTEE application. **CVE-2016-10388**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/126
NA	18-08-2017	6.9	In all Qualcomm products with Android releases from CAF using the Linux kernel, an assertion was potentially reachable in a handover scenario. **CVE-2016-10387**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/127
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, an array index out of bounds vulnerability exists in LPP.**CVE-2016-10386**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/128
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a pointer is not properly validated in a QTEE system call.**CVE-2015-9060**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/129
Overflow	22-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists when performing WCDMA radio tuning.**CVE-2015-9041**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/130
NA	22-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in a GERAN API. **CVE-2015-9040**	https://source.android.com/security/bulletin/2017-07-01	A-IBM-ANDRO-140817/131
Igniterealtime					
T-coffee					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	22-08-2017	7.6	t-coffee before 11.00.8cbe486-2 allows local users to write to ~/.t_coffee globally. **CVE-2015-8621**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=751579	A-IGN-T-COF-140817/132
Imagemagick					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an assertion was potentially reachable in a memory management routine. **CVE-2015-9055**	https://source.android.com/security/bulletin/2017-07-01	A-IMA-ANDRO-140817/133
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a NULL pointer can be dereferenced during GAL decoding.**CVE-2015-9054**	https://source.android.com/security/bulletin/2017-07-01	A-IMA-ANDRO-140817/134
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in the processing of certain responses from the USIM. **CVE-2015-9053**	https://source.android.com/security/bulletin/2017-07-01	A-IMA-ANDRO-140817/135
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in LTE where an assertion can be reached while processing a downlink message. **CVE-2015-9052**	https://source.android.com/security/bulletin/2017-07-01	A-IMA-ANDRO-140817/136
Intel					
Haproxy					
NA	18-08-2017	7.5	HAProxy statistics in openstack-tripleo-image-elements are non-authenticated over the network. **CVE-2016-2102**	https://bugzilla.redhat.com/show_bug.cgi?id=1311145	A-INT-HAPRO-140817/137
Kamailio					
Ganeti					
+Info	24-08-2017	7.6	The RESTful control interface (aka RAPI or ganeti-rapi) in Ganeti before 2.9.7, 2.10.x before 2.10.8, 2.11.x before 2.11.8,	http://docs.ganeti.org/ganeti/2.15/html/news.	A-KAM-GANET-140817/138

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			2.12.x before 2.12.6, 2.13.x before 2.13.3, 2.14.x before 2.14.2, and 2.15.x before 2.15.2 allows remote attackers to obtain the DRBD secret via instance information job results. **CVE-2015-7945**	html#version-2-15-2	
Lemur Project					
Gigacc Office					
NA	18-08-2017	7.2	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to upload arbitrary files as a user profile image, which may be exploited for unauthorized file sharing.**CVE-2016-7845**	NA	A-LEM-GIGAC-140817/139
Android					
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer over-read vulnerability exists in a TrustZone syscall. **CVE-2015-9070**	https://source.android.com/security/bulletin/2017-07-01	A-LIB-ANDRO-140817/140
Liferay					
Android					
Exec Code	17-08-2017	6.8	A remote code execution vulnerability in the Android media framework (avc decoder). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37079296.**CVE-2017-0745**	https://source.android.com/security/bulletin/2017-08-01	A-LIF-ANDRO-140817/141
Lxdm Project					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, the UE can send unprotected MeasurementReports revealing UE location.**CVE-2016-10381**	https://source.android.com/security/bulletin/2017-07-01	A-LXD-ANDRO-140817/142
Mantisbt					
Android					
Overflow	18-08-2017	7.5	In a display driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, a variable controlled by userspace is used	https://source.android.com/security/bulletin/2017-06-01	A-MAN-ANDRO-140817/143

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			to calculate offsets and sizes for copy operations, which could result in heap overflow. **CVE-2016-5861**		
Tomcat					
NA	18-08-2017	7.5	The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.**CVE-2016-0762**	NA	A-MAN-TOMCA-140817/144
Android					
NA	19-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in LTE where an assertion can be reached due to an improper bound on a length in a System Information message. **CVE-2015-9051**	https://source.android.com/security/bulletin/2017-07-01	A-MAN-ANDRO-140817/145
Mapsplugin					
Bitrix					
Exec Code Sql	23-08-2017	7.6	Multiple SQL injection vulnerabilities in the orion.extfeedbackform module before 2.1.3 for Bitrix allow remote authenticated users to execute arbitrary SQL commands via the (1) order or (2) "by" parameter to admin/orion.extfeedbackform_efbf_forms.php.**CVE-2015-8355**	NA	A-MAP-BITRI-140817/146
Zen Cart					
Dir. Trav.	23-08-2017	7.6	Directory traversal vulnerability in Zen Cart 1.5.4 allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the act parameter to ajax.php.**CVE-2015-8352**	https://www.zen-cart.com/showthread.php?218914-Security-	A-MAP-ZEN C-140817/147

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

				Patches-for-v1-5-4-November-2015	
Lxdm					
Bypass	23-08-2017	7.6	LXDM before 0.5.2 did not start X server with -auth, which allows local users to bypass authentication with X connections.**CVE-2015-8308**	https://bugzilla.redhat.com/show_bug.cgi?id=1284460	A-MAP-LXDM-140817/148
F-secure Online Scanner					
Exec Code	24-08-2017	7.6	Untrusted search path vulnerability in F-Secure Online Scanner allows remote attackers to execute arbitrary code and conduct DLL hijacking attacks via a Trojan horse DLL that is located in the same folder as F-SecureOnlineScanner.exe. **CVE-2015-8264**	https://www.f-secure.com/en/web/labs_global/fsc-2015-4	A-MAP-F-SEC-140817/149
Mod Nss Project					
Android					
Overflow	18-08-2017	7.5	In a sound driver in Android for MSM, Firefox OS for MSM, QRD Android, some variables are from userspace and values can be chosen that could result in stack overflow.**CVE-2016-5867**	https://source.android.com/security/bulletin/2017-05-01	A-MOD-ANDRO-140817/150
Sametime					
NA	18-08-2017	7.5	IBM Sametime 8.5.2 and 9.0 could store potentially sensitive information from the browser cache locally that could be available to a local user. IBM X-Force ID: 113938. **CVE-2016-2978**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-MOD-SAMET-140817/151
Modx					
Emptoris Strategic Supply Management					
+Info	18-08-2017	7.5	IBM Emptoris Strategic Supply Management Platform 10.0 and 10.1 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this	http://www.ibm.com/support/docview.wss?uid=swg22006799	A-MOD-EMPTO-140817/152

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 116881.**CVE-2016-6029**		
Mozilla					
NTP					
DoS	24-08-2017	7.8	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.**CVE-2015-7702**	http://support.ntp.org/bin/view/Main/NtpBug2899	A-MOZ-NTP-140817/153
Mpg123					
Android					
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in GNSS when performing a scan after bootup. **CVE-2015-9047**	https://source.android.com/security/bulletin/2017-07-01	A-MPG-ANDRO-140817/154
Mufg					
Android					
DoS	17-08-2017	6.8	A denial of service vulnerability in the Android media framework (libmediaplayerservice). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-38391487. **CVE-2017-0733**	https://source.android.com/security/bulletin/2017-08-01	A-MUF-ANDRO-140817/155
Musl-libc					
Sametime					
CSRF	18-08-2017	7.5	IBM Sametime Enterprise Meeting Server 8.5.2 and 9.0 could allow an authenticated user that has been invited to a Sametime meeting room, to cause the screen sharing to cease through the use of cross-site request forgery. IBM X-Force ID: 111895.**CVE-2016-0356**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-MUS-SAMET-140817/156
Netapp					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using	https://source.android.	A-NET-ANDRO-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			the Linux kernel, the use of an out-of-range pointer offset is potentially possible in LTE. **CVE-2016-10344**	com/security/bulletin/2017-07-01	140817/157
Novell					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an argument to a mink syscall is not properly validated.**CVE-2015-9068**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/158
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a potential compiler optimization of memset() is addressed. **CVE-2015-9067**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/159
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in an Inter-RAT procedure. **CVE-2015-9066**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/160
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a UE can respond to a UEInformationRequest before Access Stratum security is established.**CVE-2015-9065**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/161
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, the UE can send IMEI or IMEISV to the network on a network request before NAS security has been activated. **CVE-2015-9064**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/162
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a procedure involving a remote UIM client.**CVE-2015-9063**	https://source.android.com/security/bulletin/2017-07-01	A-NOV-ANDRO-140817/163
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, an integer overflow to buffer overflow	https://source.android.com/security/bulletin/	A-NOV-ANDRO-140817/164

			vulnerability exists when loading an ELF file.**CVE-2015-9062**	2017-07-01	
NTP					
Security Appscan					
NA	18-08-2017	7.1	IBM AppScan Enterprise Edition 9.0 contains an unspecified vulnerability that could allow an attacker to hijack a valid user's session. IBM X-Force ID: 120257 **CVE-2016-9981**	http://www.ibm.com/support/docview.wss?uid=swg22006430	A-NTP-SECUR-140817/165
Curam Social Program Management					
XSS	18-08-2017	7.1	IBM Curam Social Program Management 6.0, 6.1, 6.2 and 7.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 119761.**CVE-2016-9732**	http://www.ibm.com/support/docview.wss?uid=swg22007156	A-NTP-CURAM-140817/166
Emptoris Strategic Supply Management;Emptoris Supplier Lifecycle Management					
+Info	18-08-2017	7.1	IBM Emptoris Supplier Lifecycle Management 10.0.x and 10.1.x could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially-crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 118836. **CVE-2016-8949**	http://www.ibm.com/support/docview.wss?uid=swg22006854	A-NTP-EMPTO-140817/167
Atlas					
NA	18-08-2017	7.2	Apache Atlas versions 0.6.0 (incubating), 0.7.0 (incubating), and 0.7.1 (incubating) allow access to the webapp directory contents by pointing to URIs like	https://lists.apache.org/thread.html/f7435d66b840daa2a	A-NTP-ATLAS-140817/168

			/js and /img.**CVE-2016-8752**	38ad1329d639b70f5a9476e7580ae885d422e86@%3Cdev.atlas.apache.org%3E	
Tomcat					
+Info	18-08-2017	7.2	A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions.**CVE-2016-8745**	NA	A-NTP-TOMCA-140817/169
CXF					
NA	18-08-2017	7.2	The JAX-RS module in Apache CXF prior to 3.0.12 and 3.1.x prior to 3.1.9 provides a number of Atom JAX-RS MessageBodyReaders. These readers use Apache Abdera Parser which expands XML entities by default which represents a major XXE risk. **CVE-2016-8739**	http://cxf.apache.org/security-advisories.data/CVE-2016-8739.txt.asc	A-NTP-CXF-140817/170

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Ghostscript					
Exec Code	18-08-2017	7.2	The PS Interpreter in Ghostscript 9.18 and 9.20 allows remote attackers to execute arbitrary code via crafted userparams. **CVE-2016-7976**	https://bugs.ghostscript.com/show_bug.cgi?id=697178	A-NTP-GHOST-140817/171
Gigacc Office					
Exec Code	18-08-2017	7.2	GigaCC OFFICE ver.2.3 and earlier allows remote attackers to execute arbitrary OS commands via specially crafted mail template.**CVE-2016-7844**	NA	A-NTP-GIGAC-140817/172
Mitsubishi Ufj					
NA	18-08-2017	7.2	The Bank of Tokyo-Mitsubishi UFJ, Ltd. App for Android ver5.3.1, ver5.2.2 and earlier allow a man-in-the-middle attacker to downgrade the communication between the app and the server from TLS v1.2 to SSL v3.0, which may result in the attacker to eavesdrop on an encrypted communication. **CVE-2016-7812**	NA	A-NTP-MITSU-140817/173
Tomcat					
DoS Overflow	18-08-2017	7.2	The HTTP/2 header parser in Apache Tomcat 9.0.0.M1 to 9.0.0.M11 and 8.5.0 to 8.5.6 entered an infinite loop if a header was received that was larger than the available buffer. This made a denial of service attack possible.**CVE-2016-6817**	NA	A-NTP-TOMCA-140817/174
CXF					
XSS	18-08-2017	7.2	The HTTP transport module in Apache CXF prior to 3.0.12 and 3.1.x prior to 3.1.9 uses FormattedServiceListWriter to provide an HTML page which lists the names and absolute URL addresses of the available service endpoints. The module calculates the base URL using the current HttpServletRequest. The calculated base URL is used by FormattedServiceListWriter to build the service endpoint	https://issues.apache.org/jira/browse/CXF-6216	A-NTP-CXF-140817/175

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			absolute URLs. If the unexpected matrix parameters have been injected into the request URL then these matrix parameters will find their way back to the client in the services list page which represents an XSS risk to the client.**CVE-2016-6812**		
Tomcat					
NA	18-08-2017	7.2	The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not. **CVE-2016-6797**	NA	A-NTP-TOMCA-140817/176
Bypass	18-08-2017	7.2	A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.**CVE-2016-6796**	NA	A-NTP-TOMCA-140817/177
Onosproject					
Enterprise Virtualization					
+Info	18-08-2017	7.2	oVirt Engine discloses the ENGINE_HTTPS_PKI_TRUST_STORE_PASSWORD in /var/log/ovirt-engine/engine.log file in RHEV before 4.0.**CVE-2016-6310**	https://bugzilla.redhat.com/show_bug.cgi?id=1363738	A-ONO-ENTER-140817/178
Openjpeg					
Android					
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework	https://source.android.com/securit	A-OPE-ANDRO-140817/179

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			(libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37237701. **CVE-2017-0805**	y/bulletin/2017-08-01	
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Upstream Linux file system. Product: Android. Versions: Android kernel. Android ID: A-36817013. **CVE-2017-0750**	https://source.android.com/security/bulletin/2017-08-01	A-OPE-ANDRO-140817/180
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Upstream Linux linux kernel. Product: Android. Versions: Android kernel. Android ID: A-36007735. **CVE-2017-0749**	https://source.android.com/security/bulletin/2017-08-01	A-OPE-ANDRO-140817/181
NA	17-08-2017	6.8	A elevation of privilege vulnerability in the Qualcomm proprietary component. Product: Android. Versions: Android kernel. Android ID: A-32524214. References: QC-CR#2044821. **CVE-2017-0747**	https://source.android.com/security/bulletin/2017-08-01	A-OPE-ANDRO-140817/182
Openstack					
Sametime					
+Info	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 could allow a meeting invitee to obtain previously cleared sensitive information by viewing the meeting report history. IBM X-Force ID: 113936. **CVE-2016-2976**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-OPE-SAMET-140817/183
NA	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 could store credentials of the Sametime Meetings user in the local cache of their browser which could be accessed by a local user. IBM X-Force ID: 113855. **CVE-2016-2972**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-OPE-SAMET-140817/184
Open-uri-cached Project					
Sametime					
XSS	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 is vulnerable to cross-site scripting. This	http://www.ibm.com/support/do	A-OPE-SAMET-140817/185

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 113945. **CVE-2016-2979**	cview.wss?uid=swg22006439	
Orion-soft					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, there is a TOCTOU race condition in Secure UI.**CVE-2016-10383**	https://source.android.com/security/bulletin/2017-07-01	A-ORI-ANDRO-140817/186
Ovirt					
Android					
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37203196.**CVE-2017-0716**	https://source.android.com/security/bulletin/2017-08-01	A-OVI-ANDRO-140817/187
Phpmybackuppro					
Android					
+Info	18-08-2017	7.5	In a driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, a user-supplied buffer is casted to a structure without checking if the source buffer is large enough.**CVE-2016-5855**	https://source.android.com/security/bulletin/2017-05-01	A-PHP-ANDRO-140817/189
+Info	18-08-2017	7.5	In a driver in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, kernel heap memory can be exposed to userspace. **CVE-2016-5854**	https://source.android.com/security/bulletin/2017-05-01	A-PHP-ANDRO-140817/190
Pulp Project					
Android					
NA	18-08-2017	7.5	In an ioctl handler in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, several sanity checks are missing which can lead to out-of-bounds	https://source.android.com/security/bulletin/2017-07-01	A-PUL-ANDRO-140817/191

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			accesses.**CVE-2016-5863**		
Puppetlabs					
Android					
Exec Code	18-08-2017	6.8	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37561455.**CVE-2017-0721**	https://source.android.com/security/bulletin/2017-08-01	A-PUP-ANDRO-140817/192
Qemu					
Android					
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer over-read vulnerability exists in digital television/digital radio DRM.**CVE-2015-8595**	https://source.android.com/security/bulletin/2017-07-01	A-QEM-ANDRO-140817/193
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer over-read vulnerability exists in RFA-1x.**CVE-2015-8594**	https://source.android.com/security/bulletin/2017-07-01	A-QEM-ANDRO-140817/194
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in 1x call processing. **CVE-2015-8593**	https://source.android.com/security/bulletin/2017-07-01	A-QEM-ANDRO-140817/195
Redhat					
Android					
NA	18-08-2017	6.8	A elevation of privilege vulnerability in the Android media framework (libgui). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-33004354.**CVE-2017-0727**	https://source.android.com/security/bulletin/2017-08-01	A-RED-ANDRO-140817/196
DoS	18-08-2017	6.8	A denial of service vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-36389123. **CVE-2017-0726**	https://source.android.com/security/bulletin/2017-08-01	A-RED-ANDRO-140817/197
Overflow	22-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer over-	https://source.android.com/securit	A-RED-ANDRO-140817/198

			read may occur in the processing of a downlink 3G NAS message. **CVE-2015-9037**	y/bulletin/ 2017-07-01	
Mem. Corr.	23-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a pointer is not validated prior to being dereferenced potentially resulting in Guest-OS memory corruption.**CVE-2015-8592**	https://source.android.com/security/bulletin/2017-07-01	A-RED-ANDRO-140817/199
Rest-client Project					
Sametime					
NA	18-08-2017	7.5	IBM Sametime 8.5.2 and 9.0 could allow an unauthorized authenticated user to enumerate group chat ID numbers and join meetings that he was not invited to. IBM X-Force ID: 111928. **CVE-2016-0358**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-RES-SAMET-140817/191
Restkit					
Sametime					
NA	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 may send replies that contain emails of people that should not be in these messages. IBM X-Force ID: 113850. **CVE-2016-2969**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-RES-SAMET-140817/192
Saltstack					
Emptoris Strategic Supply Management;Emptoris Supplier Lifecycle Management					
XSS	18-08-2017	7.2	IBM Emptoris Supplier Lifecycle Management 10.0.x and 10.1.x is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 118383. **CVE-2016-6121**	http://www.ibm.com/support/docview.wss?uid=swg22006854	A-SAL-EMPTO-140817/193
Android					
+Info	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, kernel stack data can be leaked to userspace by an audio driver.	https://source.android.com/security/bulletin/2017-05-01	A-SAL-ANDRO-140817/194

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE-2016-5347		
Smartcms					
Android					
NA	20-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists where an array out of bounds access can occur during a CA call.**CVE-2015-9050**	https://source.android.com/security/bulletin/2017-07-01	A-SMA-ANDRO-140817/195
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in the processing of certain responses from the USIM. **CVE-2015-9049**	https://source.android.com/security/bulletin/2017-07-01	A-SMA-ANDRO-140817/196
Snapcreek					
Android					
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a NULL pointer can be dereferenced upon the expiry of a timer. **CVE-2015-9043**	https://source.android.com/security/bulletin/2017-07-01	A-SNA-ANDRO-140817/197
Sugarcrm					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, arguments to several QTEE syscalls are not properly validated. **CVE-2016-5872**	https://source.android.com/security/bulletin/2017-07-01	A-SUG-ANDRO-140817/198
Tcoffee					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, an assertion was potentially reachable in a WLAN driver ioctl. **CVE-2016-10384**	https://source.android.com/security/bulletin/2017-07-01	A-TCO-ANDRO-140817/199
Telescopeapp					
Android					
Overflow	22-08-2017	7.6	In all Qualcomm products with Android releases from CAF using the Linux kernel, a memory buffer fails to be freed after it is no longer needed potentially	https://source.android.com/security/bulletin/2017-07-01	A-TEL-ANDRO-140817/200

			resulting in memory exhaustion. **CVE-2015-9035**		
Trendmicro					
Android					
DoS	18-08-2017	6.8	A denial of service vulnerability in the Android media framework (libskia). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-37627194. **CVE-2017-0725**	https://source.android.com/security/bulletin/2017-08-01	A-TRE-ANDRO-140817/201
Unit4					
Android					
Overflow	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer over-read vulnerability exists in a TrustZone syscall. **CVE-2015-9071**	https://source.android.com/security/bulletin/2017-07-01	A-UNI-ANDRO-140817/202
Unshield Project					
Manageengine Opmanager					
NA	18-08-2017	7.5	Zoho ManageEngine OpManager 11 through 12.2 uses a custom encryption algorithm to protect the credential used to access the monitored devices. The implemented algorithm doesn't use a per-system key or even a salt; therefore, it's possible to create a universal decryptor. **CVE-2015-9107**	https://github.com/theguly/DecryptOpManager	A-UNS-MANAG-140817/203
Util-linux Project					
Android					
Overflow	18-08-2017	7.5	In an audio driver function in all Qualcomm products with Android for MSM, Firefox OS for MSM, or QRD Android, some parameters are from userspace, and if they are set to a large value, integer overflow is possible followed by buffer overflow. In another function, a missing check for a lower bound may result in an out of bounds memory access. **CVE-2016-5864**	https://source.android.com/security/bulletin/2017-06-01	A-UTI-ANDRO-140817/204
Vbulletin					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Android					
Overflow	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in GERAN where a buffer can be overflown while taking power measurements. **CVE-2015-9045**	https://source.android.com/security/bulletin/2017-07-01	A-VBU-ANDRO-140817/205
W1.fi					
Android					
NA	18-08-2017	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, playReady DRM failed to check a length potentially leading to unauthorized access to secure memory.**CVE-2015-9061**	https://source.android.com/security/bulletin/2017-07-01	A-W1.-ANDRO-140817/206
Web-dorado					
Android					
NA	2017-08-21	7.5	In all Qualcomm products with Android releases from CAF using the Linux kernel, a vulnerability exists in LTE where an assertion can be reached due to an improper bound on the size of a frequency list.**CVE-2015-9044**	https://source.android.com/security/bulletin/2017-07-01	A-WEB-ANDRO-140817/207
X.org					
NTP					
DoS	24-08-2017	7.8	Memory leak in the CRYPTO_ASSOC function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (memory consumption). **CVE-2015-7701**	https://bugzilla.redhat.com/show_bug.cgi?id=1274255	A-X.O-NTP-140817/208
Xymon					
Sametime					
NA	18-08-2017	7.5	IBM Sametime Enterprise Meeting Server 8.5.2 and 9.0 could allow an authenticated user to upload a malicious file to a Sametime meeting room, that could be downloaded by unsuspecting users which could be executed with user privileges. IBM X-Force ID: 111893.	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-XYM-SAMET-140817/209

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE-2016-0354		
Yeager					
Tomcat					
Bypass +Info	18-08-2017	7.2	When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible.**CVE-2016-6794**	NA	A-YEA-TOMCA-140817/210
Zen-cart					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using the Linux kernel, access control to the I2C bus is not sufficient. **CVE-2016-10382**	https://source.android.com/security/bulletin/2017-07-01	A-ZEN-ANDRO-140817/211
Zend					
Sametime					
NA	18-08-2017	7.5	IBM Sametime Meeting Server 8.5.2 and 9.0 could allow a malicious user to lower other users hands in the meeting. IBM X-Force ID: 113937. **CVE-2016-2977**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-ZEN-SAMET-140817/212
CSRF	18-08-2017	7.5	IBM Sametime Enterprise Meeting Server 8.5.2 and 9.0 could allow an authenticated user that has been invited to a Sametime meeting room, to cause the screen sharing to cease through the use of cross-site request forgery. IBM X-Force ID: 111894.**CVE-2016-0355**	http://www.ibm.com/support/docview.wss?uid=swg22006439	A-ZEN-SAMET-140817/213
Zohocorp					
Android					
NA	18-08-2017	7.1	In all Qualcomm products with Android releases from CAF using	https://source.android.	A-ZOH-ANDRO-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			the Linux kernel, a use-after-free vulnerability exists in IMS RCS. **CVE-2016-10385**	com/security/bulletin/2017-07-01	140817/214
Sametime					
XSS	18-08-2017	7.5	IBM Sametime 8.5.2 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Sametime away message altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 113848.**CVE-2016-2967**	http://www.ibm.com/support/docview.wss?uid=swg22006441	A-ZOH-SAMET-140817/215
Zope					
NTP					
DoS	24-08-2017	7.8	The ntpd client in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service via a number of crafted "KOD" messages. **CVE-2015-7704**	https://bugzilla.redhat.com/show_bug.cgi?id=1271070	A-ZOP-NTP-140817/216
Entrouvert/Fedoraproject					
NTP					
DoS	24-08-2017	7.8	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.**CVE-2015-7692**	https://bugzilla.redhat.com/show_bug.cgi?id=1274254	A-ENT-NTP-140817/217
Qemu/Redhat					
NTP					
DoS	24-08-2017	7.8	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted packets containing particular autokey operations. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.**CVE-2015-7691**	https://bugzilla.redhat.com/show_bug.cgi?id=1274254	A-QEM-NTP-140817/218
Hardware (H)					
Citrix					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Yeager Cms					
Exec Code	24-08-2017	7.8	Unrestricted file upload vulnerability in Yeager CMS 1.2.1 allows remote attackers to execute arbitrary code by uploading a file with an executable extension. **CVE-2015-7571**	NA	H-CIT-YEAGE-140817/219
Operating System (OS)					
Canonical					
Graphviz					
DoS Exec Code Overflow	30-08-2017	10	Stack-based buffer overflow in the "yyerror" function in Graphviz 2.34.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted file. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-0978. **CVE-2014-1235**	https://bugzilla.redhat.com/show_bug.cgi?id=1050871	O-CAN-GRAPH-140817/220
Qemu					
DoS	30-08-2017	10	The qcow2_open function in the (block/qcow2.c) in QEMU before 1.7.2 and 2.x before 2.0.0 allows local users to cause a denial of service (NULL pointer dereference) via a crafted image which causes an error, related to the initialization of the snapshot_offset and nb_snapshots fields. **CVE-2014-0146**	http://git.qemu.org/?p=qemu.git;a=commit;h=11b128f4062dd7f89b14abc8877ff20d41b28be9	O-CAN-QEMU-140817/221
Cisco					
Busybox					
Dir. Trav.	31-08-2017	10	Directory traversal vulnerability in the BusyBox implementation of tar before 1.22.0 v5 allows remote attackers to point to files outside the current working directory via a symlink. **CVE-2011-5325**	https://bugzilla.redhat.com/show_bug.cgi?id=1274215	O-CIS-BUSYB-140817/222
Fortinet					
Express					
XSS	29-08-2017	10	The Express web framework before 3.11 and 4.x before 4.5 for	https://nodesecurity.io	O-FOR-EXPRE-140817/223

			Node.js does not provide a charset field in HTTP Content-Type headers in 400 level responses, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via characters in a non-standard encoding.**CVE-2014-6393**	/advisories /express-no-charset-in-content-type-header	
Security Network Protection 3100 Firmware;Security Network Protection 4100 Firmware;Security Network Protection 5100 Firmware;Security Network Protection 7100 Firmware					
XSS	30-08-2017	10	Cross-site scripting (XSS) vulnerability in IBM Security Network Protection 3100, 4100, 5100, and 7100 devices with firmware 5.2 before 5.2.0.0-ISS-XGS-All-Models-Hotfix-FP0008 and 5.3 before 5.3.0.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. **CVE-2014-6189**	http://www-01.ibm.com/support/docview.wss?uid=swg21697248	O-FOR-SECUR-140817/224
Telescope					
XSS	30-08-2017	10	Cross-site scripting (XSS) vulnerability in Telescope before 0.9.3 allows remote authenticated users to inject arbitrary web script or HTML via crafted markdown. **CVE-2014-5144**	http://www.telescopeapp.org/blog/telescope-v093-dailyscope/	O-FOR-TELES-140817/225
Good For Enterprise					
XSS	30-08-2017	10	Cross-site scripting (XSS) vulnerability in Good for Enterprise for Android 2.8.0.398 and 1.9.0.40.**CVE-2014-4925**	NA	O-FOR-GOOD -140817/226
Google					
Kubernetes/Openshift					
NA	24-08-2017	7.8	Kubernetes in OpenShift3 allows remote authenticated users to use the private images of other users should they know the name of said image. **CVE-2015-7561**	https://github.com/kubernetes/kubernetes/pull/18909	O-GOO-KUBER-140817/227
Onos					
DoS	25-08-2017	7.8	ONOS before 1.5.0 when using the ifwd app allows remote attackers to cause a denial of	https://wiki.onosproject.org/display	O-GOO-ONOS-140817/228

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			service (NULL pointer dereference and switch disconnect) by sending two Ethernet frames with ether_type Jumbo Frame (0x8870). **CVE-2015-7516**	/ONOS/Security+advisories	
Zxv10 W300 Firmware					
NA	25-08-2017	7.8	ZTE ADSL ZXV10 W300 modems W300V2.1.0f_ER7_PE_O57 and W300V2.1.0h_ER7_PE_O57 allow user accounts to have multiple valid username and password pairs, which allows remote authenticated users to login to a target account via any of its username and password pairs. **CVE-2015-7259**	NA	O-GOO-ZXV10-140817/229
Zxv10 W300 Firmware					
+Info	25-08-2017	7.8	ZTE ADSL ZXV10 W300 modems W300V2.1.0f_ER7_PE_O57 and W300V2.1.0h_ER7_PE_O57 allow remote authenticated users to obtain user passwords by displaying user information in a Telnet connection. **CVE-2015-7258**	NA	O-GOO-ZXV10-140817/230
Zxv10 W300 Firmware					
NA	25-08-2017	7.8	ZTE ADSL ZXV10 W300 modems W300V2.1.0f_ER7_PE_O57 and W300V2.1.0h_ER7_PE_O57 allow remote authenticated non-administrator users to change the admin password by intercepting an outgoing password change request, and changing the username parameter from "support" to "admin".**CVE-2015-7257**	NA	O-GOO-ZXV10-140817/231
Coremail Xt					
XSS	25-08-2017	7.8	Cross-site scripting (XSS) vulnerability in Coremail XT3.0 allows remote attackers to inject arbitrary web script or HTML via a hyperlink in a document attachment.**CVE-2015-6942**	http://seclists.org/fulldisclosure/2015/Nov/100	O-GOO-COREM-140817/232
Salt 2015					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

+Info	25-08-2017	7.8	win_useradd, salt-cloud and the Linode driver in salt 2015.5.x before 2015.5.6, and 2015.8.x before 2015.8.1 leak password information in debug logs. **CVE-2015-6941**	https://github.com/twangboy/salt/commit/c0689e32154c41f59840ae10ffc5fbfa30618710	O-GOO-SALT -140817/234
Fedora/Ganglia-web					
Bypass	25-08-2017	7.8	ganglia-web before 3.7.1 allows remote attackers to bypass authentication.**CVE-2015-6816**	https://bugzilla.redhat.com/show_bug.cgi?id=1260562	O-GOO-FEDOR-140817/235
Modx Revolution					
XSS	25-08-2017	7.8	Cross-site scripting (XSS) vulnerability in login-fsp.html in MODX Revolution before 1.9.1 allows remote attackers to inject arbitrary web script or HTML via the QUERY_STRING. **CVE-2015-6588**	http://packetstormsecurity.com/files/134529/MODX-2.3.5-Cross-Site-Scripting.html	O-GOO-MODX -140817/236
Home Device Manager					
NA	25-08-2017	8.3	Alcatel-Lucent Home Device Manager before 4.1.10, 4.2.x before 4.2.2 allows remote attackers to spoof and make calls as target devices. **CVE-2015-6498**	NA	O-GOO-HOME -140817/237
Wago I/o Plc 750-849 Firmware;Wago I/o Plc 758-870 Firmware					
NA	25-08-2017	8.3	WAGO IO 750-849 01.01.27 and WAGO IO 750-881 01.02.05 do not contain privilege separation. **CVE-2015-6473**	NA	O-GOO-WAGO -140817/238
Wago I/o Plc 750-849 Firmware;Wago I/o Plc 750-881 Firmware;Wago I/o Plc 758-870 Firmware					
NA	25-08-2017	8.3	WAGO IO 750-849 01.01.27 and 01.02.05, WAGO IO 750-881, and WAGO IO 758-870 have weak credential management. **CVE-2015-6472**	NA	O-GOO-WAGO -140817/239
Sugarcrm					
Exec Code	25-08-2017	8.5	Incomplete blacklist vulnerability in SuiteCRM 7.2.2 allows remote authenticated	NA	O-GOO-SUGAR-140817/240

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			users to execute arbitrary code by uploading a file with an executable extension. **CVE-2015-5946**		
Logstash					
+Info	25-08-2017	9	Logstash 1.4.x before 1.4.5 and 1.5.x before 1.5.4 with Lumberjack output or the Logstash forwarder does not validate SSL/TLS certificates from the Logstash server, which might allow attackers to obtain sensitive information via a man-in-the-middle attack. **CVE-2015-5619**	https://www.elastic.co/blog/logstash-1-5-4-and-1-4-5-released	O-GOO-LOGST-140817/241
Fedora/Spring Social					
CSRF	25-08-2017	9	Cross-site request forgery (CSRF) vulnerability in springframework-social before 1.1.3.**CVE-2015-5258**	https://bugzilla.redhat.com/show_bug.cgi?id=1305443	O-GOO-FEDOR-140817/242
Mod Nss					
Bypass	25-08-2017	9	The NSSCipherSuite option with ciphersuites enabled in mod_nss before 1.0.12 allows remote attackers to bypass application restrictions.**CVE-2015-5244**	https://pagure.io/mod_nss/c/34e1ccecb4a7d5054dba2f92b403af9b6ae1e110	O-GOO-MOD N-140817/243
Util-linux					
NA	25-08-2017	9	The mkostemp function in login-utils in util-linux when used incorrectly allows remote attackers to cause file name collision and possibly other attacks.**CVE-2015-5224**	https://bugzilla.redhat.com/show_bug.cgi?id=1256686	O-GOO-UTIL--140817/244
Fedora/Leap;Opensuse/Jasper					
DoS	25-08-2017	9	Double free vulnerability in the jasper_image_stop_load function in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.**CVE-2015-5203**	https://bugzilla.redhat.com/show_bug.cgi?id=1254242	O-GOO-FEDOR-140817/245
Pulp					
+Priv	26-08-2017	9	Pulp does not remove permissions for named objects	https://bugzilla.redhat.	O-GOO-PULP-140817/246

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			upon deletion, which allows authenticated users to gain the privileges of a deleted object via creating an object with the same name.**CVE-2015-5153**	com/show_bug.cgi?id=1243526	
Django Cms					
CSRF	28-08-2017	9.3	Cross-site request forgery (CSRF) vulnerability in django CMS before 3.0.14, 3.1.x before 3.1.1 allows remote attackers to manipulate privileged users into performing unknown actions via unspecified vectors. **CVE-2015-5081**	https://www.django-cms.org/en/blog/2015/06/27/311-3014-release/	O-GOO-DJANG-140817/247
Mantisbt					
+Info	28-08-2017	9.3	The "Project Documentation" feature in MantisBT 1.2.19 and earlier, when the threshold to access files ($g_view_proj_doc_threshold) is set to ANYBODY, allows remote authenticated users to download attachments linked to arbitrary private projects via a file id number in the file_id parameter to file_download.php. **CVE-2015-5059**	https://bugzilla.redhat.com/show_bug.cgi?id=1237199	O-GOO-MANTI-140817/248
Broken Link Checker					
XSS	28-08-2017	9.3	Cross-site scripting (XSS) vulnerability exists in the Wordpress admin panel when the Broken Link Checker plugin before 1.10.9 is installed. **CVE-2015-5057**	NA	O-GOO-BROKE-140817/249
Splash Portal					
XSS	28-08-2017	9.3	Cross-site scripting (XSS) vulnerability in the Splash Portal in Cloud4Wi before 5.9.7 allows remote attackers to inject arbitrary web script or HTML via the recoveryMessage parameter to the default URI. **CVE-2015-4699**	https://cloud4wi.zendesk.com/hc/en-us/articles/204956829-Cloud4Wi-5-9-7-Release-Note	O-GOO-SPLAS-140817/250
Clearpass					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

+Priv	28-08-2017	9.3	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote authenticated administrators to gain root privileges via unspecified vectors, a different vulnerability than CVE-2015-3654.**CVE-2015-4649**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/251
Kg-sha104 Firmware;Kg-sha108 Firmware					
NA	28-08-2017	9.3	Kguard Digital Video Recorder 104, 108, v2 does not have any authorization or authentication between an ActiveX client and the application server. **CVE-2015-4464**	NA	O-GOO-KG-SH-140817/252
Phpmybackuppro					
Dir. Trav.	28-08-2017	9.3	Directory traversal vulnerability in get_file.php in phpMyBackupPro 2.1 through 2.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the view parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: this vulnerability exists due to an incomplete fix to CVE-2015-4180.**CVE-2015-4181**	http://www.openwall.com/lists/oss-security/2015/06/04/10	O-GOO-PHPMY-140817/253
Dir. Trav.	28-08-2017	9.3	Directory traversal vulnerability in get_file.php in phpMyBackupPro 2.1 through 2.4 allows remote attackers to read arbitrary files via a .. (dot dot) in the view parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information. NOTE: this vulnerability exists due to an incomplete fix to CVE-2009-4050.**CVE-2015-4180**	http://www.openwall.com/lists/oss-security/2015/06/04/10	O-GOO-PHPMY-140817/254
Elasticsearch					
Exec Code	28-08-2017	9.3	The snapshot API in Elasticsearch before 1.6.0 when another application exists on the system that can read Lucene files	https://www.elastic.co/community/security/	O-GOO-ELAST-140817/256

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			and execute code from them, is accessible by the attacker, and the Java VM on which Elasticsearch is running can write to a location that the other application can read and execute from, allows remote authenticated users to write to and create arbitrary snapshot metadata files, and potentially execute arbitrary code. **CVE-2015-4165**		
Attic					
+Info	28-08-2017	9.3	attic before 0.15 does not confirm unencrypted backups with the user, which allows remote attackers with read and write privileges for the encrypted repository to obtain potentially sensitive information by changing the manifest type byte of the repository to "unencrypted / without key file". **CVE-2015-4082**	https://github.com/jborg/attic/issues/271	O-GOO-ATTIC-140817/257
Helpdesk Pro					
+Info	28-08-2017	9.3	The Helpdesk Pro Plugin before 1.4.0 for Joomla! allows remote attackers to read the support tickets of arbitrary users via obtaining the target ticketId, and navigating to http://{target}/component/helpdeskpro/?view=ticket&id={ticketId}.**CVE-2015-4071**	NA	O-GOO-HELPD-140817/258
Salt					
NA	28-08-2017	9.3	Salt before 2014.7.6 does not verify certificates when connecting via the aliyun, proxmox, and splunk modules. **CVE-2015-4017**	https://docs.saltstack.com/en/latest/topics/releases/2014.7.6.html	O-GOO-SALT-140817/259
Android					
DoS	28-08-2017	9.3	The updateMessageStatus function in Android 5.1.1 and earlier allows local users to cause a denial of service (NULL pointer exception and process	https://huntcve.github.io/2017/02/13/cveupdate/	O-GOO-ANDRO-140817/260

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			crash).**CVE-2015-3839**		
Clearpass					
+Priv	28-08-2017	9.3	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote authenticated lower-level administrators to gain "Super Admin" privileges via unspecified vectors. **CVE-2015-3657**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/261
+Priv	28-08-2017	9.3	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote authenticated lower-level administrators to gain privileges by leveraging failure to properly enforce authorization checks. **CVE-2015-3656**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/262
CSRF	28-08-2017	9.3	Cross-site request forgery (CSRF) vulnerability in Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote attackers to hijack the authentication of administrators by leveraging improper enforcement of the anti-CSRF token.**CVE-2015-3655**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/263
+Priv	28-08-2017	9.3	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote authenticated administrators to gain root privileges via unspecified vectors, a different vulnerability than CVE-2015-4649.**CVE-2015-3654**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/264
DoS +Priv	28-08-2017	9.3	Aruba Networks ClearPass Policy Manager before 6.4.7 and 6.5.x before 6.5.2 allows remote authenticated administrators to write to arbitrary files within the underlying operating system and consequently cause a denial of service or gain privileges by leveraging incorrect permission checking.**CVE-2015-3653**	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2015-009.txt	O-GOO-CLEAR-140817/265
Fortimanager Firmware					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Exec Code Sql	28-08-2017	9.3	SQL injection vulnerability in Fortinet FortiManager 5.0.x before 5.0.11, 5.2.x before 5.2.2 allows remote attackers to execute arbitrary commands via unspecified parameters. **CVE-2015-3616**	https://fortiguard.com/psirt/FG-IR-15-011	O-GOO-FORTI-140817/266
XSS	28-08-2017	9.3	Cross-site scripting (XSS) vulnerability in Fortinet FortiManager 5.0.x before 5.0.11, 5.2.x before 5.2.2 allows remote authenticated users to inject arbitrary web script or HTML via vectors involving unspecified parameters and a privilege escalation attack. **CVE-2015-3615**	https://fortiguard.com/psirt/FG-IR-15-011	O-GOO-FORTI-140817/267
+Info	28-08-2017	9.3	Fortinet FortiManager 5.0.x before 5.0.11, 5.2.x before 5.2.2 allows remote attackers to obtain arbitrary files via vectors involving another unspecified vulnerability.**CVE-2015-3614**	https://fortiguard.com/psirt/FG-IR-15-011	O-GOO-FORTI-140817/268
Debian Linux/Fedora/Suse Linux Enterprise Server/Suse Linux Enterprise Desktop/Enterprise Linux Desktop;Enterprise Linux For Ibm Z Systems;Enterprise Linux For Power Big Endian;Enterprise Linux For Scientific Computing;Enterprise Linux Server;Enterprise Linux Server From Rhui 6;Enterprise Linux Workstation/Suse Linux Enterprise Server/NTP					
NA	28-08-2017	9.3	ntp-keygen in ntp 4.2.8px before 4.2.8p2-RC2 and 4.3.x before 4.3.12 does not generate MD5 keys with sufficient entropy on big endian machines when the lowest order byte of the temp variable is between 0x20 and 0x7f and not #, which might allow remote attackers to obtain the value of generated MD5 keys via a brute force attack with the 93 possible keys. **CVE-2015-3405**	https://bugzilla.redhat.com/show_bug.cgi?id=1210324	O-GOO-DEBIA-140817/269
Mod Nss					
+Info	28-08-2017	9.3	The mod_nss module before 1.0.11 in Fedora allows remote attackers to obtain cipher lists due to incorrect parsing of multi-keyword cipherstring. **CVE-2015-3277**	https://bugzilla.redhat.com/show_bug.cgi?id=1238324	O-GOO-MOD N-140817/270

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Diactoros					
XSS	28-08-2017	9.3	Zend/Diactoros/Uri::filterPath in zend-diactoros before 1.0.4 does not properly sanitize path input, which allows remote attackers to perform cross-site scripting (XSS) or open redirect attacks. **CVE-2015-3257**	https://framework.zend.com/security/advisory/ZF2015-05	O-GOO-DIACT-140817/271
Trove					
NA	28-08-2017	9.3	The _write_config function in trove/guestagent/datastore/experimental/mongodb/service.py, reset_configuration function in trove/guestagent/datastore/experimental/postgresql/service/config.py, write_config function in trove/guestagent/datastore/experimental/redis/service.py, _write_mycnf function in trove/guestagent/datastore/mysql/service.py, InnoBackupEx::_run_prepare function in trove/guestagent/strategies/restore/mysql_impl.py, InnoBackupEx::cmd function in trove/guestagent/strategies/backup/mysql_impl.py, MySQLDump::cmd in trove/guestagent/strategies/backup/mysql_impl.py, InnoBackupExIncremental::cmd function in trove/guestagent/strategies/backup/mysql_impl.py, _get_actual_db_status function in trove/guestagent/datastore/experimental/cassandra/system.py and trove/guestagent/datastore/experimental/cassandra/service.py, and multiple class CbBackup methods in trove/guestagent/strategies/backup/experimental/couchbase_impl.py in Openstack DBaaS (aka Trove) as packaged in Openstack	https://bugzilla.redhat.com/show_bug.cgi?id=1216073	O-GOO-TROVE-140817/272

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			before 2015.1.0 (aka Kilo) allows local users to write to configuration files via a symlink attack on a temporary file. **CVE-2015-3156**		
File Transfer Appliance					
Exec Code	28-08-2017	9.3	Accellion File Transfer Appliance before FTA_9_11_210 allows remote attackers to execute arbitrary code via shell metacharacters in the oauth_token parameter. **CVE-2015-2857**	NA	O-GOO-FILE - 140817/273
Addons Module					
XSS	28-08-2017	9.3	Multiple cross-site scripting (XSS) vulnerabilities in views/add-license-form.php in the Digium Addons module (digiumaddoninstaller) before 2.11.0.7 for FreePBX allow remote attackers to inject arbitrary web script or HTML via the (1) add_license_key, (2) add_license_first_name, (3) add_license_last_name, (4) add_license_company, (5) add_license_address1, (6) add_license_address2, (7) add_license_city, (8) add_license_state, (9) add_license_post_code, (10) add_license_country, (11) add_license_phone, or (12) add_license_email parameter in an add-license-form page to admin/config.php. **CVE-2015-2690**	http://git.freepbx.org/projects/FREEPBX/repos/digiumaddoninstaller/commits/2aad006024b74c9ff53943d3e68527a3dffac855	O-GOO-ADDON-140817/274
Compute					
NA	28-08-2017	9.3	OpenStack Compute (nova) Icehouse, Juno and Havana when live migration fails allows local users to access VM volumes that they would normally not have permissions for.**CVE-2015-2687**	https://bugs.launchpad.net/nova/+bug/1419577	O-GOO-COMPU-140817/275
Librest					
DoS Overflow	28-08-2017	9.3	The OAuth implementation in librest before 0.7.93 incorrectly	https://bugzilla.redhat.	O-GOO-LIBRE-140817/276

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			truncates the pointer returned by the rest_proxy_call_get_url function, which allows remote attackers to cause a denial of service (application crash) via running the EnsureCredentials method from the org.gnome.OnlineAccounts.Account interface on an object representing a Flickr account. **CVE-2015-2675**	com/show_bug.cgi?id=1183982	
Restkit					
NA	28-08-2017	9.3	Restkit allows man-in-the-middle attackers to spoof TLS servers by leveraging use of the ssl.wrap_socket function in Python with the default CERT_NONE value for the cert_reqs argument. **CVE-2015-2674**	https://bugzilla.redhat.com/show_bug.cgi?id=1202837	O-GOO-RESTK-140817/277
Manageengine Desktop Central					
NA	28-08-2017	9.3	Manage Engine Desktop Central 9 before build 90135 allows remote attackers to change passwords of users with the Administrator role via an addOrModifyUser operation to servlets/DCOperationsServlet. **CVE-2015-2560**	https://www.manageengine.com/products/desktop-central/unauthorized-admin-credential-modification.html	O-GOO-MANAG-140817/278
Capnproto					
DoS	28-08-2017	9.3	Sandstorm Cap'n Proto before 0.4.1.1 and 0.5.x before 0.5.1.2, when an application invokes the totalSize method on an object reader, allows remote peers to cause a denial of service (CPU consumption) via a crafted small message, which triggers a "tight" for loop. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-2312.**CVE-2015-2313**	https://github.com/capnproto/capnproto/blob/master/security-advisories/2015-03-05-0-c%2B%2B-addl-cpu-amplification.md	O-GOO-CAPNP-140817/279
DoS	28-08-2017	9.3	Sandstorm Cap'n Proto before	https://gith	O-GOO-CAPNP-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			0.4.1.1 and 0.5.x before 0.5.1.1 allows remote peers to cause a denial of service (CPU and possibly general resource consumption) via a list with a large number of elements. **CVE-2015-2312**	ub.com/capnproto/capnproto/commit/104870608fde3c698483fdef6b97f093fc15685d	140817/280
DoS Exec Code +Info	28-08-2017	9.3	Integer underflow in Sandstorm Cap'n Proto before 0.4.1.1 and 0.5.x before 0.5.1.1 might allow remote peers to cause a denial of service or possibly obtain sensitive information from memory or execute arbitrary code via a crafted message. **CVE-2015-2311**	https://github.com/capnproto/capnproto/commit/26bcceda72372211063d62aab7e45665faa83633	O-GOO-CAPNP-140817/281
DoS Overflow +Info	28-08-2017	9.3	Integer overflow in layout.c++ in Sandstorm Cap'n Proto before 0.4.1.1 and 0.5.x before 0.5.1.1 allows remote peers to cause a denial of service or possibly obtain sensitive information from memory via a crafted message, related to pointer validation.**CVE-2015-2310**	https://github.com/capnproto/capnproto/commit/f343f0dbd0a2e87f17cd74f14186ed73e3fbdbfa	O-GOO-CAPNP-140817/282
Ethernet Diagnostics Driver Iqvw32.sys;Ethernet Diagnostics Driver Iqvw64.sys					
DoS Exec Code	28-08-2017	9.3	(1) IQVW32.sys before 1.3.1.0 and (2) IQVW64.sys before 1.3.1.0 in the Intel Ethernet diagnostics driver for Windows allows local users to cause a denial of service or possibly execute arbitrary code with kernel privileges via a crafted (a) 0x80862013, (b) 0x8086200B, (c) 0x8086200F, or (d) 0x80862007 IOCTL call. **CVE-2015-2291**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00051&languageid=en-fr	O-GOO-ETHER-140817/283
Mantisbt					
XSS	28-08-2017	9.3	Cross-site scripting (XSS) vulnerability in MantisBT 1.2.13 and later before 1.2.20. **CVE-2015-2046**	https://bugzilla.redhat.com/show_bug.cgi?id=1191130	O-GOO-MANTI-140817/284
Rest-client					
+Info	28-08-2017	9.3	REST client for Ruby (aka rest-	https://bug	O-GOO-REST--

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			client) before 1.8.0 allows remote attackers to conduct session fixation attacks or obtain sensitive cookie information by leveraging passage of cookies set in a response to a redirect. **CVE-2015-1820**	zilla.redhat.com/show_bug.cgi?id=1205291	140817/285
Musl					
Overflow	28-08-2017	9.3	Stack-based buffer overflow in the inet_pton function in network/inet_pton.c in musl libc 0.9.15 through 1.0.4, and 1.1.0 through 1.1.7 allows attackers to have unspecified impact via unknown vectors. **CVE-2015-1817**	NA	O-GOO-MUSL-140817/286
Galaxy S4 Firmware					
DoS Overflow +Priv Mem. Corr.	28-08-2017	9.3	The samsung_extdisp driver in the Samsung S4 (GT-I9500) I9500XXUEMK8 kernel 3.4 and earlier allows attackers to cause a denial of service (memory corruption) or gain privileges. **CVE-2015-1801**	NA	O-GOO-GALAX-140817/287
+Info	28-08-2017	9.3	The samsung_extdisp driver in the Samsung S4 (GT-I9500) I9500XXUEMK8 kernel 3.4 and earlier allows attackers to potentially obtain sensitive information.**CVE-2015-1800**	NA	O-GOO-GALAX-140817/288
Lasso/Fedora					
DoS Overflow	28-08-2017	9.3	The prefix variable in the get_or_define_ns function in Lasso before commit 6d854cef4211cdcdbc7446c978f23ab859847cdd allows remote attackers to cause a denial of service (uninitialized memory access and application crash) via unspecified vectors. **CVE-2015-1783**	https://bugzilla.redhat.com/show_bug.cgi?id=1199925	O-GOO-LASSO-140817/289
Zend Framework					
NA	28-08-2017	9.3	Zend/Session/SessionManager in Zend Framework 2.2.x before 2.2.9, 2.3.x before 2.3.4 allows remote attackers to create valid sessions without using session	http://framework.zend.com/security/advisory/ZF2015-01	O-GOO-ZEND -140817/290

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			validators.**CVE-2015-1555**		
Xymon					
Overflow	28-08-2017	9.3	Buffer overflow in xymon 4.3.17-1. **CVE-2015-1430**	http://www.openwall.com/lists/oss-security/2015/01/31/4	O-GOO-XYMON-140817/291
Ubuntu Linux/Fedora/Patch					
Dir. Trav.	28-08-2017	9.3	Directory traversal vulnerability in GNU patch versions which support Git-style patching before 2.7.3 allows remote attackers to write to arbitrary files with the permissions of the target user via a .. (dot dot) in a diff file name. **CVE-2015-1395**	https://savannah.gnu.org/bugs/?44059	O-GOO-UBUNT-140817/292
Unshield					
Dir. Trav.	28-08-2017	9.3	Directory traversal vulnerability in unshield 1.0-1. **CVE-2015-1386**	https://bugzilla.redhat.com/show_bug.cgi?id=1185717	O-GOO-UNSHI-140817/293
Grml-debootstrap					
NA	28-08-2017	9.3	cmdlineopts.clp in grml-debootstrap in Debian 0.54, 0.68.x before 0.68.1, 0.7x before 0.78 is sourced without checking that the local directory is writable by non-root users. **CVE-2015-1378**	https://github.com/grml/grml-debootstrap/issues/59	O-GOO-GRML--140817/294
Ubuntu Linux					
+Priv	28-08-2017	9.3	Race condition in Apport before 2.17.2-0ubuntu1.1 as packaged in Ubuntu 15.04, before 2.14.70ubuntu8.5 as packaged in Ubuntu 14.10, before 2.14.1-0ubuntu3.11 as packaged in Ubuntu 14.04 LTS, and before 2.0.1-0ubuntu17.9 as packaged in Ubuntu 12.04 LTS allow local users to write to arbitrary files and gain root privileges. **CVE-2015-1325**	NA	O-GOO-UBUNT-140817/295
Exponent Cms					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

XSS	28-08-2017	9.3	Cross-site scripting (XSS) vulnerability in Exponent CMS 2.3.2.**CVE-2015-1177**	NA	O-GOO-EXPON-140817/296
Teta Web					
NA	28-08-2017	9.3	Session fixation vulnerability in Unit4 Polska TETA Web (formerly TETA Galactica) 22.62.3.4 and earlier allows remote attackers to hijack web sessions via a session id. **CVE-2015-1174**	http://packetstormsecurity.com/files/133296/UNIT4TETA-TETA-WEB-22.62.3.4-Session-Fixation.html	O-GOO-TETA -140817/297
Libhtp					
DoS	28-08-2017	9.3	libhtp 0.5.15 allows remote attackers to cause a denial of service (NULL pointer dereference).**CVE-2015-0928**	NA	O-GOO-LIBHT-140817/298
Linux Imaging And Printing					
Exec Code	28-08-2017	9.3	The hp-plugin utility in HP Linux Imaging and Printing (HPLIP) makes it easier for man-in-the-middle attackers to execute arbitrary code by leveraging use of a short GPG key id from a keyserver to verify print plugin downloads.**CVE-2015-0839**	https://bugzilla.redhat.com/show_bug.cgi?id=1227252	O-GOO-LINUX-140817/299
Zenworks Configuration Management					
Exec Code Overflow	28-08-2017	9.3	Stack-based buffer overflow in the logging functionality in the Preboot Policy service in Novell ZENworks Configuration Management (ZCM) allows remote attackers to execute arbitrary code via unspecified vectors.**CVE-2015-0786**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/300
+Info	28-08-2017	9.3	com.novell.zenworks.inventory.rtr.actionclasses.wcreports in Novell ZENworks Configuration Management (ZCM) allows remote attackers to read arbitrary folders via the dirname variable.**CVE-2015-0785**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/301
+Info	28-08-2017	9.3	Rtrlet.class in Novell ZENworks Configuration Management	https://www.novell.co	O-GOO-ZENWO-

			(ZCM) allows remote attackers to obtain Session IDs of logged in users via a value of ShowLogins for the maintenance variable. **CVE-2015-0784**	m/support/kb/doc.php?id=7016431	140817/302
+Info	28-08-2017	9.3	The FileViewer class in Novell ZENworks Configuration Management (ZCM) allows remote authenticated users to read arbitrary files via the filename variable. **CVE-2015-0783**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/304
Exec Code Sql	28-08-2017	9.3	SQL injection vulnerability in the ScheduleQuery method of the schedule class in Novell ZENworks Configuration Management (ZCM) allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **CVE-2015-0782**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/305
Dir. Trav.	28-08-2017	9.3	Directory traversal vulnerability in the doPost method of the Rtrlet class in Novell ZENworks Configuration Management (ZCM) allows remote attackers to upload and execute arbitrary files via unspecified vectors. **CVE-2015-0781**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/306
Exec Code Sql	28-08-2017	10	SQL injection vulnerability in the GetReRequestData method of the GetStoredResult class in Novell ZENworks Configuration Management (ZCM) allows remote attackers to execute arbitrary SQL commands via unspecified vectors. **CVE-2015-0780**	https://www.novell.com/support/kb/doc.php?id=7016431	O-GOO-ZENWO-140817/307
Android					
Overflow	28-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in HSDPA.**CVE-2015-0576**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/308
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, insecure	https://source.android.com/securit	O-GOO-ANDRO-140817/309

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			ciphersuites were included in the default configuration. **CVE-2015-0575**	y/bulletin/ 2017-07-01	
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, the validation of filesystem access was insufficient.**CVE-2015-0574**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/310
Wpa Supplicant					
NA	29-08-2017	10	wpa_supplicant 2.0-16 does not properly check certificate subject name, which allows remote attackers to cause a man-in-the-middle attack.**CVE-2015-0210**	https://bugzilla.redhat.com/show_bug.cgi?id=1178921	O-GOO-WPA S-140817/311
Sterling B2b Integrator;Sterling File Gateway					
NA	29-08-2017	10	XML External Entity (XXE) vulnerability in IBM Sterling B2B Integrator 5.1 and 5.2 and IBM Sterling File Gateway 2.1 and 2.2 allows remote attackers to read arbitrary files via a crafted XML data.**CVE-2015-0194**	http://www-01.ibm.com/support/docview.wss?uid=swg21699482	O-GOO-STERL-140817/312
Android					
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, an overflow check in the USB interface was insufficient during boot. **CVE-2014-9981**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/313
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a Sample App failed to check a length potentially leading to unauthorized access to secure memory.**CVE-2014-9980**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/314
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a variable is uninitialized in a TrustZone system call potentially leading to the compromise of secure memory.**CVE-2014-9979**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/315
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in a	https://source.android.com/security/bulletin/	O-GOO-ANDRO-140817/316

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			QTEE service. **CVE-2014-9978**	2017-07-01	
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in PlayReady DRM.**CVE-2014-9977**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/317
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in 1x call processing. **CVE-2014-9976**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/318
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a rollback vulnerability potentially exists in Full Disk Encryption. **CVE-2014-9975**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/319
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, validation of buffer lengths was missing in Keymaster.**CVE-2014-9974**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/320
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, validation of a buffer length was missing in a PlayReady DRM routine. **CVE-2014-9973**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/321
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, disabling asserts can potentially cause a NULL pointer dereference during an out-of-memory condition. **CVE-2014-9972**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/322
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, disabling asserts causes an instruction inside of an assert to not be executed resulting in incorrect control flow.**CVE-2014-9971**	https://source.android.com/security/bulletin/2017-07-01	O-GOO-ANDRO-140817/323
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, the GPS client	https://source.android.com/securit	O-GOO-ANDRO-140817/324

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			may use an insecure cryptographic algorithm. **CVE-2014-9969**	y/bulletin/ 2017-07-01	
Overflow	29-08-2017	10	In all Qualcomm products with Android releases from CAF using the Linux kernel, a buffer overflow vulnerability exists in the UIMDIAG interface. **CVE-2014-9968**	https://source.android.com/security/bulletin/ 2017-07-01	O-GOO-ANDRO-140817/325
Imagemagick					
NA	29-08-2017	10	coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file. **CVE-2014-9831**	https://bugzilla.redhat.com/show_bug.cgi?id=1343487	O-GOO-IMAGE-140817/326
NA	29-08-2017	10	coders/sun.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted sun file.**CVE-2014-9830**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=b68b78e2625122d9f6b6d88ba4df7e85b47b556f	O-GOO-IMAGE-140817/327
NA	29-08-2017	10	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file.**CVE-2014-9828**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=460547be494cc8c039b99b65e64a1fa2eb08ab5c	O-GOO-IMAGE-140817/328

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	29-08-2017	10	coders/xpm.c in ImageMagick allows remote attackers to have unspecified impact via a crafted xpm file. **CVE-2014-9827**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=69490f5cffbda612e15a2985699455bb0b45e276	O-GOO-IMAGE-140817/329
Mantisbt					
XSS	29-08-2017	10	Cross-site scripting (XSS) vulnerability in MantisBT before 1.2.19 and 1.3.x before 1.3.0-beta.2 allows remote attackers to inject arbitrary web script or HTML via the url parameter to permalink_page.php. **CVE-2014-9701**	https://www.mantisbt.org/bugs/view.php?id=17362#c40613	O-GOO-MANTI-140817/330
Ubuntu Linux/Fedora/Mageia/Patch					
DoS	29-08-2017	10	GNU patch 2.7.2 and earlier allows remote attackers to cause a denial of service (memory consumption and segmentation fault) via a crafted diff file. **CVE-2014-9637**	https://savannah.gnu.org/bugs/?44051	O-GOO-UBUNT-140817/331
En6131 Firmware;Ib6131 Firmware					
XSS Http R.Spl. +Info	29-08-2017	10	CRLF injection vulnerability in IBM Flex System EN6131 40Gb Ethernet and IB6131 40Gb Infiniband Switch firmware before 3.4.1110 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks and resulting web cache poisoning or cross-site scripting (XSS) attacks, or obtain sensitive information via multiple unspecified parameters.**CVE-2014-9564**	https://www.ibm.com/support/home/docdisplay?lndocid=MIGR-5098173	O-GOO-EN613-140817/332
Smartcms					

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

Vulnerability Type(s):

DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

Sql	29-08-2017	10	Multiple SQL injection vulnerabilities in SmartCMS v.2. **CVE-2014-9558**	NA	O-GOO-SMART-140817/333
XSS	29-08-2017	10	Multiple cross-site scripting (XSS) vulnerabilities in SmartCMS v.2.**CVE-2014-9557**	NA	O-GOO-SMART-140817/334
Footprints Service Core					
XSS	29-08-2017	10	Cross-site scripting (XSS) vulnerability in BMC Footprints Service Core 11.5. **CVE-2014-9514**	http://www.securityfocus.com/archive/1/534648	O-GOO-FOOTP-140817/335
Mpg123					
Overflow	29-08-2017	10	Buffer overflow in mpg123 before 1.18.0.**CVE-2014-9497**	NA	O-GOO-MPG12-140817/336
Emacs					
Bypass	29-08-2017	10	Emacs 24.4 allows remote attackers to bypass security restrictions. **CVE-2014-9483**	https://bugzilla.redhat.com/show_bug.cgi?id=1181599	O-GOO-EMACS-140817/337
Vbulletin					
XSS	29-08-2017	10	Cross-site scripting (XSS) vulnerability in vBulletin 3.5.4, 3.6.0, 3.6.7, 3.8.7, 4.2.2, 5.0.5, and 5.1.3. **CVE-2014-9469**	NA	O-GOO-VBULL-140817/338
Satellite					
NA	29-08-2017	10	Red Hat Satellite 6 allows local users to access mongod and delete pulp_database. **CVE-2014-8168**	https://bugzilla.redhat.com/show_bug.cgi?id=1192249	O-GOO-SATEL-140817/339
Qemu					
DoS Exec Code Overflow	30-08-2017	10	Multiple buffer overflows in QEMU before 1.7.2 and 2.x before 2.0.0, allow local users to cause a denial of service (crash) or possibly execute arbitrary code via a large (1) L1 table in the qcow2_snapshot_load_tmp in the QCOW 2 block driver (block/qcow2-snapshot.c) or (2) uncompressed chunk, (3) chunk length, or (4) number of sectors in the DMG block driver	https://bugzilla.redhat.com/show_bug.cgi?id=1078885	O-GOO-QEMU-140817/340

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			(block/dmg.c).**CVE-2014-0145**		
Qemu/Enterprise Linux					
DoS Overflow Mem. Corr.	30-08-2017	10	Multiple integer overflows in the block drivers in QEMU, possibly before 2.0.0, allow local users to cause a denial of service (crash) via a crafted catalog size in (1) the parallels_open function in block/parallels.c or (2) bochs_open function in bochs.c, a large L1 table in the (3) qcow2_snapshot_load_tmp in qcow2-snapshot.c or (4) qcow2_grow_l1_table function in qcow2-cluster.c, (5) a large request in the bdrv_check_byte_request function in block.c and other block drivers, (6) crafted cluster indexes in the get_refcount function in qcow2-refcount.c, or (7) a large number of blocks in the cloop_open function in cloop.c, which trigger buffer overflows, memory corruption, large memory allocations and out-of-bounds read and writes. **CVE-2014-0143**	https://bugzilla.redhat.com/show_bug.cgi?id=1079140	O-GOO-QEMU/-140817/341
Qemu					
DoS	30-08-2017	10	QEMU, possibly before 2.0.0, allows local users to cause a denial of service (divide-by-zero error and crash) via a zero value in the (1) tracks field to the seek_to_sector function in block/parallels.c or (2) extent_size field in the bochs function in block/bochs.c. **CVE-2014-0142**	https://bugzilla.redhat.com/show_bug.cgi?id=1078201	O-GOO-QEMU-140817/342
Satellite					
XSS	30-08-2017	10	Cross-site scripting (XSS) vulnerability in Red Hat Satellite 6.0.3. **CVE-2014-0141**	https://bugzilla.redhat.com/show_bug.cgi?id=1187466	O-GOO-SATEL-140817/343
Googlemaps					

CV Scoring Scale (CVSS)	**0-1**	**1-2**	**2-3**	**3-4**	**4-5**	**5-6**	**6-7**	**7-8**	**8-9**	**9-10**
Vulnerability Type(s): **DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable**										

XSS	30-08-2017	10	Cross-site scripting (XSS) vulnerability in the Googlemaps plugin before 3.1 for Joomla!. **CVE-2013-7433**	http://www.mapsplugin.com/Google-Maps/Documentation-of-plugin-Googlemap/security-release-3-1-of-plugin-googlemaps.html	O-GOO-GOOGL-140817/344
Bypass	30-08-2017	10	The Googlemaps plugin before 3.1 for Joomla! allows remote attackers to bypass an intended protection mechanism. **CVE-2013-7432**	http://www.mapsplugin.com/Google-Maps/Documentation-of-plugin-Googlemap/security-release-3-1-of-plugin-googlemaps.html	O-GOO-GOOGL-140817/345
NA	30-08-2017	10	Full path disclosure in the Googlemaps plugin before 3.1 for Joomla!. **CVE-2013-7431**	http://www.mapsplugin.com/Google-Maps/Documentation-of-plugin-Googlemap/security-release-3-1-of-plugin-googlemaps.html	O-GOO-GOOGL-140817/346
XSS	31-08-2017	10	Cross-site scripting (XSS) vulnerability in the Googlemaps plugin before 3.1 for Joomla! allows remote attackers to inject arbitrary web script or HTML via the xmlns parameter. **CVE-2013-7430**	http://www.mapsplugin.com/Google-Maps/Documentation-of-plugin-Googlemap/	O-GOO-GOOGL-140817/347

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

				security-release-3-1-of-plugin-googlemaps.html	
Kamailio					
NA	31-08-2017	10	Insecure Temporary file vulnerability in /tmp/kamailio_fifo in kamailio 4.0.1. **CVE-2013-7426**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=712083	O-GOO-KAMAI-140817/348
Ffmpeg					
NA	31-08-2017	10	The 'vp3_decode_frame' function in FFmpeg 1.1.4 moves threads check out of header packet type check. **CVE-2013-0870**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/349
IOS					
DoS	31-08-2017	10	Cisco IOS before 15.2(4)S6 does not initialize an unspecified variable, which might allow remote authenticated users to cause a denial of service (CPU consumption, watchdog timeout, crash) by walking specific SNMP objects. **CVE-2012-5030**	https://www.cisco.com/c/en/us/td/docs/ios/15_2s/release/notes/15_2s_rel_notes/15_2s_caveats_15_24s.html	O-GOO-IOS-140817/350
Ffmpeg					
DoS	31-08-2017	10	Unspecified vulnerability in FFMPEG 0.10 allows remote attackers to cause a denial of service. **CVE-2012-2805**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/351
NA	31-08-2017	10	Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2778, and CVE-2012-2780. **CVE-2012-2781**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/352
NA	31-08-2017	10	Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2778, and CVE-2012-2781. **CVE-2012-2780**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/353

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

NA	31-08-2017	10	Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2773, CVE-2012-2780, and CVE-2012-2781. **CVE-2012-2778**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/354
NA	31-08-2017	10	Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2771, CVE-2012-2778, CVE-2012-2780, and CVE-2012-2781. **CVE-2012-2773**	https://www.ffmpeg.org/security.html	O-GOO-FFMPE-140817/356
Xerces-c++					
DoS	31-08-2017	10	Apache Xerces-C++ allows remote attackers to cause a denial of service (CPU consumption) via a crafted message sent to an XML service that causes hash table collisions. **CVE-2012-0880**	https://bugzilla.redhat.com/show_bug.cgi?id=787103	O-GOO-XERCE-140817/357
IBM					
Ffmpeg					
NA	31-08-2017	10	Unspecified vulnerability in FFmpeg before 0.10.3 has unknown impact and attack vectors, a different vulnerability than CVE-2012-2773, CVE-2012-2778, CVE-2012-2780, and CVE-2012-2781. **CVE-2012-2771**	https://www.ffmpeg.org/security.html	O-IBM-FFMPE-140817/358
CXF					
Bypass	31-08-2017	10	The WS-SP UsernameToken policy in Apache CXF 2.4.5 and 2.5.1 allows remote attackers to bypass authentication by sending an empty UsernameToken as part of a SOAP request. **CVE-2012-0803**	http://svn.apache.org/viewvc?view=revision&revision=1233457	O-IBM-CXF-140817/359
Kguardsecurity					
Load Balancer					
NA	29-08-2017	10	Hard coded weak credentials in Barracuda Load Balancer 5.0.0.015. **CVE-2014-8426**	NA	O-KGU-LOAD -140817/360
Linux					
Myfaces					

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

+Info	31-08-2017	10	Information disclosure vulnerability in Apache MyFaces Core 2.0.1 through 2.0.10 and 2.1.0 through 2.1.4 allows remote attackers to inject EL expressions via crafted parameters. **CVE-2011-4343**	https://issues.apache.org/jira/secure/attachment/12504807/MYFACES-3405-1.patch	O-LIN-MYFAC-140817/361
Microsoft					
Open-uri-cached					
Exec Code	28-08-2017	9.3	The open-uri-cached rubygem allows local users to execute arbitrary Ruby code by creating a directory under /tmp containing "openuri-" followed by a crafted UID, and putting Ruby code in said directory once a meta file is created. **CVE-2015-3649**	NA	O-MIC-OPEN--140817/362
Netscaler Application Delivery Controller;Netscaler Gateway					
+Info	28-08-2017	9.3	The TLS and DTLS processing functionality in Citrix NetScaler Application Delivery Controller (ADC) and NetScaler Gateway devices with firmware 9.x before 9.3 Build 68.5, 10.0 through Build 78.6, 10.1 before Build 130.13, 10.1.e before Build 130.1302.e, 10.5 before Build 55.8, and 10.5.e before Build 55.8007.e makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, a variant of CVE-2014-3566 (aka POODLE). **CVE-2015-3642**	http://support.citrix.com/article/CTX200378	O-MIC-NETSC-140817/363
Fortimanager Firmware					
+Priv	28-08-2017	9.3	Fortinet FortiManager 5.0 before 5.0.11 and 5.2 before 5.2.2 allow local users to gain privileges via crafted CLI commands. **CVE-2015-3617**	https://fortiguard.com/psirt/FG-IR-15-011	O-MIC-FORTI-140817/364
Samsung					
Android					
NA	29-08-2017	10	In all Qualcomm products with Android releases from CAF using	https://source.android.	O-SAM-ANDRO-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			the Linux kernel, the use of an out-of-range pointer offset is potentially possible in rollback protection. **CVE-2014-9411**	com/security/bulletin/2017-07-01	140817/365
Photo Gallery					
NA	29-08-2017	10	Unrestricted File Upload vulnerability in Photo Gallery 1.2.5. **CVE-2014-9312**	NA	O-SAM-PHOTO-140817/366
Leap;Opensuse/Encfs					
+Info	30-08-2017	10	The ".encfs6.xml" configuration file in encfs before 1.7.5 allows remote attackers to access sensitive data by setting "blockMACBytes" to 0 and adding 8 to "blockMACRandBytes". **CVE-2014-3462**	https://bugzilla.redhat.com/show_bug.cgi?id=1097537	O-SAM-LEAP;-140817/367
Openfire					
NA	30-08-2017	10	OpenFire XMPP Server before 3.10 accepts self-signed certificates, which allows remote attackers to perform unspecified spoofing attacks. **CVE-2014-3451**	NA	O-SAM-OPENF-140817/368
Suse					
Data Center Network Manager					
NA	31-08-2017	10	Cisco Data Center Network Manager is affected by Excessive Logging During a TCP Flood on Java Ports. If the size of server.log becomes very big because of too much logging by the DCNM server, then the CPU utilization increases. Known Affected Releases: 5.2(1). Known Fixed Releases: 6.0(0)SL1(0.14) 5.2(2.73)S0. Product identification: CSCtt15295. **CVE-2011-4650**	https://quickview.cloudapps.cisco.com/quickview/bug/CSCtt15295	O-SUS-DATA -140817/369
Wago					
Urbancode Deploy					
CSRF	29-08-2017	10	Cross-site request forgery (CSRF) vulnerability in IBM UrbanCode Release 6.0.1.6 and earlier, 6.1.0.7 and earlier, and 6.1.1.1 and earlier.	http://www-01.ibm.com/support/docview.wss?	O-WAG-URBAN-140817/370

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			CVE-2014-8900	uid=swg21695293	
Load Balancer					
NA	29-08-2017	10	Privilege escalation vulnerability in Barracuda Load Balancer 5.0.0.015 via the use of an improperly protected SSH key. **CVE-2014-8428**	NA	O-WAG-LOAD -140817/371
Westermo					
Ubuntu Linux					
+Priv	28-08-2017	9.3	Apport before 2.17.2-0ubuntu1.1 as packaged in Ubuntu 15.04, before 2.14.70ubuntu8.5 as packaged in Ubuntu 14.10, before 2.14.1-0ubuntu3.11 as packaged in Ubuntu 14.04 LTS, and before 2.0.1-0ubuntu17.9 as packaged in Ubuntu 12.04 LTS allow local users to write to arbitrary files and gain root privileges by leveraging incorrect handling of permissions when generating core dumps for setuid binaries. **CVE-2015-1324**	https://bugs.launchpad.net/ubuntu/+source/apport/+bug/1452239	O-WES-UBUNT-140817/372
ZTE					
Duplicator					
NA	29-08-2017	10	The Duplicator plugin in Wordpress before 0.5.10 allows remote authenticated users to create and download backup files. **CVE-2014-9262**	https://www.exploit-db.com/exploits/36112/	O-ZTE-DUPLI-140817/373
Download Manager					
NA	29-08-2017	10	The basic_settings function in the download manager plugin for WordPress before 2.7.3 allows remote authenticated users to update every WordPress option. **CVE-2014-9260**	http://packetstormsecurity.com/files/130690/WordPress-Download-Manager-2.7.2-Privilege-Escalation.html	O-ZTE-DOWNL-140817/374
Curam Social Program Management					
NA	29-08-2017	10	IBM Curam Social Program	http://ww	O-ZTE-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			Management 6.0 SP2 before EP26, 6.0.4 before 6.0.4.5iFix10 and 6.0.5 before 6.0.5.6 allows remote authenticated users to load arbitrary Java classes via unspecified vectors. **CVE-2014-8903**	w-01.ibm.com/support/docview.wss?uid=swg21700098	CURAM-140817/375
Operating System; Application (OS/A)					
Canonical;Fedoraproject/GNU					
Firefox					
Exec Code Overflow	31-08-2017	10	Remote code execution in the Venkman script debugger in Mozilla Firefox before 2.0.0.8. **CVE-2007-5341**	https://bugzilla.suse.com/show_bug.cgi?id=332512	O-CAN-FIREF-140817/376
Libxfont					
Overflow	31-08-2017	10	A single byte overflow in catalogue.c in X.Org libXfont 1.3.1 allows remote attackers to have unspecified impact. **CVE-2007-5199**	https://cgit.freedesktop.org/xorg/lib/libXfont/commit/?id=5bf703700ee4a5d6eae20da07cb7a29369667aef	O-CAN-LIBXF-140817/377
Debian;Fedoraproject;Opensuse;Opensuse Project;Redhat;Suse/NTP					
Zope					
XSS	31-08-2017	10	Cross-site scripting (XSS) vulnerability in ZMI pages that use the manage_tabs_message in Zope 2.11.4, 2.11.2, 2.10.9, 2.10.7, 2.10.6, 2.10.5, 2.10.4, 2.10.2, 2.10.1, 2.12. **CVE-2009-5145**	https://bugs.launchpad.net/zope2/+bug/490514	O-DEB-ZOPE-140817/378
Fedoraproject/Ganglia					
Opensuse					
NA	31-08-2017	10	Code injection in openSUSE when running some source services used in the open build service 2.1 before March 11 2011. **CVE-2011-0469**	NA	O-FED-OPENS-140817/379
Fedoraproject/Pivotal Software					
Apache Authenhook					
+Info	31-08-2017	10	libapache-authenhook-perl 2.00-	https://rt.c	O-FED-APACH-

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable

			04 stores usernames and passwords in plaintext in the vhost error log. **CVE-2010-3845**	pan.org/Public/Bug/Display.html?id=62040	140817/380
Fedoraproject;Opensuse Project/Jasper Project					
Wink					
DoS	31-08-2017	10	XML External Entity (XXE) vulnerability in Apache Wink 1.1.1 and earlier allows remote attackers to read arbitrary files or cause a denial of service via a crafted XML document. **CVE-2010-2245**	https://svn.apache.org/repos/asf/wink/trunk/security/CVE-2010-2245.pdf	O-FED-WINK-140817/381
Opensuse Project/Vgough					
Linux Kernel					
DoS Overflow	31-08-2017	10	The ia64 subsystem in the Linux kernel before 2.6.26 allows local users to cause a denial of service (stack consumption and system crash) via a crafted application that leverages the mishandling of invalid Register Stack Engine (RSE) state. **CVE-2006-3635**	https://github.com/torvalds/linux/commit/4dcc29e1574d88f4465ba865ed82800032f76418	O-OPE-LINUX-140817/382

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

Vulnerability Type(s):
DoS- Denial of Service; CSRF-Cross Site Request Forgery; XSS- Cross Site Scripting; Sql- SQL Injection; NA: Not Applicable