National Critical Information Infrastructure Protection Centre

CVE Report

01-15 April 2017 **Vol. 04 No. 06**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Apache					
Ambari The Apache Ambari project is aimed at making Hadoop management simpler by developing software for provisioning, managing, and monitoring Apache Hadoop clusters.					
NA	03-04-2017	7.5	During installation of Ambari 2.4.0 through 2.4.2, Ambari Server artifacts are not created with proper ACLs. **CVE ID: CVE-2017-5642**	https://cwiki.apache.org/confluence/display/AMBARI/Ambari+Vulnerabilities#AmbariVulnerabilities-FixedinAmbari2.5.0	A-APA-AMBAR-200417/01
Geode Apache Geode provides a database-like consistency model, reliable transaction processing and a shared-nothing architecture to maintain very low latency performance with high concurrency processing.					
Gain Information	04-04-2017	4	Apache Geode before 1.1.1, when a cluster has enabled security by setting the security-manager property, allows remote authenticated users with CLUSTER:READ but not DATA:READ permission to access the data browser page in Pulse and consequently execute an OQL query that exposes data stored in the cluster. **CVE ID: CVE-2017-5649**	NA	A-APA-GEODE-200417/02
Ignite Apache Ignite is an in-memory computing platform that delivers unprecedented speed and unlimited scale to modern data processing.					
NA	07-04-2017	4.3	Apache Ignite before 1.9 allows man-in-the-middle attackers to read arbitrary files via XXE in modified update-notifier documents. **CVE ID: CVE-2016-6805**	http://seclists.org/oss-sec/2017/q2/31	A-APA-IGNIT-200417/03
Tika					

Apache Tika is a content detection and analysis framework, written in Java, stewarded at the Apache Software Foundation					
Execute Code	06-04-2017	7.5	Apache Tika before 1.14 allows Java code execution for serialized objects embedded in MATLAB files. The issue exists because Tika invokes JMatIO to do native deserialization. **CVE ID: CVE-2016-6809**	http://seclists.org/bugtraq/2016/Nov/40	A-APA-TIKA-200417/04
Tomcat Apache Tomcat, often referred to as Tomcat Server, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF).					
Execute Code	06-04-2017	7.5	Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types. **CVE ID: CVE-2016-8735**	http://seclists.org/oss-sec/2016/q4/502	A-APA-TOMCA-200417/05
Apple					
Apple Music Apple Music is a music-streaming service, developed by Apple Inc.					
Gain Information	07-04-2017	2.9	The Apple Music (aka com.apple.android.music) application before 2.0 for Android does not verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate. **CVE ID: CVE-2017-2387**	https://support.apple.com/HT207605	A-APP-APPLE-200417/06
Icloud; Itunes iCloud makes sure you always have the latest versions of your most important things (documents, photos, notes, contacts, and more) on all your devices; iTunes is the world's best way to play and add to your collection of music, movies, TV shows, apps, audiobooks, and more, right on your Mac or PC.					
NA	01-04-2017	3.5	An issue was discovered in certain Apple products. iCloud	https://support.apple.co	A-APP-ICLOU-

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 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. The issue involves cleartext client-certificate transmission in the "APNs Server" component. It allows man-in-the-middle attackers to track users via correlation with this certificate. **CVE ID: CVE-2017-2383**	m/HT207607	200417/07
Keynote; Numbers; Pages The three apps for both iOS and OS X that form Apple's iWork suite (Pages,Numbers, and Keynote), will be made available on a web interface (named asPages for iCloud, Numbers for iCloud, and Keynote for iCloud respectively), and accessed via the iCloud website under each users iCloud Apple ID login.					
Bypass	01-04-2017	5	An issue was discovered in certain Apple products. Pages before 6.1, Numbers before 4.1, and Keynote before 7.1 on macOS and Pages before 3.1, Numbers before 3.1, and Keynote before 3.1 on iOS are affected. The issue involves the "Export" component. It allows users to bypass iWork PDF password protection by leveraging use of 40-bit RC4. **CVE ID: CVE-2017-2391**	https://support.apple.com/HT207595	A-APP-KEYNO-200417/08
Safari Safari is a web browser developed by Apple based on the WebKit engine.					
Gain Information	01-04-2017	2.1	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "Safari Login AutoFill" component. It allows local users to obtain access to locked keychain items via unspecified vectors. **CVE ID: CVE-2017-2385**	https://support.apple.com/HT207600	A-APP-SAFAR-200417/09
DoS	03-04-2017	5	JavaScriptCore in WebKit, as distributed in Safari Technology Preview Release 18, allows remote attackers to cause a denial of service (bitfield out-of-bounds read and application crash) via crafted JavaScript code that is mishandled in the	https://trac.webkit.org/changeset/209295	A-APP-SAFAR-200417/10

			operatorString function, related to assembler/MacroAssemblerARM64.h, assembler/MacroAssemblerX86Common.h, and wasm/WasmB3IRGenerator.cpp. **CVE ID: CVE-2016-10226**		
DoS	03-04-2017	5	runtime/JSONObject.cpp in JavaScriptCore in WebKit, as distributed in Safari Technology Preview Release 18, allows remote attackers to cause a denial of service (segmentation violation and application crash) via crafted JavaScript code that triggers a "type confusion" in the JSON.stringify function. **CVE ID: CVE-2016-10222**	http://trac.webkit.org/changeset/208123	A-APP-SAFAR-200417/11
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2392**	https://support.apple.com/HT207600	A-APP-SAFAR-200417/12
DoS	03-04-2017	7.5	JavaScriptCore in WebKit, as distributed in Safari Technology Preview Release 22, allows remote attackers to cause a denial of service (heap-based out-of-bounds write and application crash) or possibly have unspecified other impact via crafted JavaScript code that triggers access to red-zone memory locations, related to jit/ThunkGenerators.cpp, llint/LowLevelInterpreter32_64.asm, and llint/LowLevelInterpreter64.asm. **CVE ID: CVE-2017-5949**	https://bugs.webkit.org/show_bug.cgi?id=167239	A-APP-SAFAR-200417/13

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

Apt-cacher Project; Apt-cacher-ng Project					
Apt-cacher/Apt-cacher-ng Apt-Cacher-NG is a caching proxy server (or apt proxy) for Debian based distributions like Ubuntu, Kubuntu, Xubuntu, Edubuntu, Linux Mint, etc, which is used to cache the downloaded packages locally on your server.					
Http Response Splitting	05-04-2017	4.3	apt-cacher before 1.7.15 and apt-cacher-ng before 3.4 allow HTTP response splitting via encoded newline characters, related to lack of blocking for the %0[ad] regular expression. **CVE ID: CVE-2017-7443**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=858833	A-APT-APT-C-200417/14
Artifex					
Ghostscript Ghostscript is a suite of software based on an interpreter for Adobe Systems' PostScript and Portable Document Format (PDF) page description languages.					
DoS	03-04-2017	4.3	The mem_get_bits_rectangle function in base/gdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file. **CVE ID: CVE-2017-5951**	https://bugs.ghostscript.com/show_bug.cgi?id=697548	A-ART-GHOST-200417/15
DoS	03-04-2017	4.3	The gs_makewordimagedevice function in base/gsdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file that is mishandled in the PDF Transparency module. **CVE ID: CVE-2016-10220**	https://bugs.ghostscript.com/show_bug.cgi?id=697450	A-ART-GHOST-200417/16
DoS	03-04-2017	4.3	The intersect function in base/gxfill.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file. **CVE ID: CVE-2016-10219**	https://bugs.ghostscript.com/show_bug.cgi?id=697453	A-ART-GHOST-200417/17
DoS	03-04-2017	4.3	The pdf14_pop_transparency_group	https://bugs.ghostscript.c	A-ART-GHOST-

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

			function in base/gdevp14.c in the PDF Transparency module in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file. **CVE ID: CVE-2016-10218**	om/show_bug.cgi?id=697444	200417/18
DoS	03-04-2017	4.3	The pdf14_open function in base/gdevp14.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted file that is mishandled in the color management module. **CVE ID: CVE-2016-10217**	https://bugs.ghostscript.com/show_bug.cgi?id=697456	A-ART-GHOST-200417/19
DoS; Overflow	03-04-2017	6.8	The fill_threshhold_buffer function in base/gxht_thresh.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document. **CVE ID: CVE-2016-10317**	NA	A-ART-GHOST-200417/20
Mupdf MuPDF is a lightweight PDF, XPS, and E-book viewer. MuPDF consists of a software library, command line tools, and viewers for various platforms.					
DoS; Overflow	03-04-2017	4.3	The count_entries function in pdf-layer.c in Artifex Software, Inc. MuPDF 1.10a allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted PDF document. **CVE ID: CVE-2016-10221**	https://bugs.ghostscript.com/show_bug.cgi?id=697400	A-ART-MUPDF-200417/21
Atlassian					
Bitbucket Bitbucket is a web-based hosting service for source code and development projects that use either Mercurial (since launch) or Git (since October 2011) revision control systems that is owned by					

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**										

Atlassian.					
Directory Traversal	09-04-2017	4	Atlassian Bitbucket Server before 4.7.1 allows remote attackers to read the first line of an arbitrary file via a directory traversal attack on the pull requests resource. **CVE ID: CVE-2016-4320**	NA	A-ATL-BITBU-200417/22
Confluence Confluence is a team collaboration software. Written in Java and mainly used in corporate environments, it is developed and marketed by Atlassian.					
XSS	09-04-2017	3.5	Atlassian Confluence Server before 5.9.11 has XSS on the viewmyprofile.action page. **CVE ID: CVE-2016-4317**	NA	A-ATL-CONFL-200417/23
Jira Jira (stylized JIRA) is a proprietary issue tracking product, developed by Atlassian.					
XSS	09-04-2017	3.5	Atlassian JIRA Server before 7.1.9 has XSS in project/ViewDefaultProjectRoleActors.jspa via a role name. **CVE ID: CVE-2016-4318**	NA	A-ATL-JIRA-200417/24
CSRF	09-04-2017	6.8	Atlassian JIRA Server before 7.1.9 has CSRF in auditing/settings. **CVE ID: CVE-2016-4319**	NA	A-ATL-JIRA-200417/25
DoS; Execute Code	10-04-2017	7.5	The JIRA Workflow Designer Plugin in Atlassian JIRA Server before 6.3.0 improperly uses an XML parser and deserializer, which allows remote attackers to execute arbitrary code, read arbitrary files, or cause a denial of service via a crafted serialized Java object. **CVE ID: CVE-2017-5983**	https://jira.atlassian.com/browse/JRASERVER-64077	A-ATL-JIRA-200417/26
Auromeera					
Emli eMLi provides integration of best-in-class technologies for improved management of the organization and secure access.					
XSS	11-04-2017	4.3	Cross Site Scripting Vulnerability in core-eMLi in AuroMeera Technometrix Pvt. Ltd. eMLi V1.0 allows an Attacker to send malicious code, generally in the form of a	https://sudoat.blogspot.in/2017/04/xss-vulnerability-in-multiple-	A-AUR-EMLI-200417/27

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

			browser-side script, to a different end user via the page parameter to code/student_portal/home.php. The affected versions are eMLi School Management 1.0, eMLi College Campus Management 1.0, and eMLi University Management 1.0. **CVE ID: CVE-2017-7621**	emli.html	
Backintime Project					
Backintime Back In Time is a simple backup tool for Linux, inspired by "flyback project".					
NA	06-04-2017	9.3	The _checkPolkitPrivilege function in serviceHelper.py in Back In Time (aka backintime) 1.1.18 and earlier uses a deprecated polkit authorization method (unix-process) that is subject to a race condition (time of check, time of use). With this authorization method, the owner of a process requesting a polkit operation is checked by polkitd via /proc/<pid>/status, by which time the requesting process may have been replaced by a different process with the same PID that has different privileges then the original requester. **CVE ID: CVE-2017-7572**	https://github.com/bit-team/backintime/commit/7f208dc547f569b689c888103e3b593a48cd1869	A-BAC-BACKI-200417/28
Bigtreecms					
Bigtree Cms BigTree CMS is an open source content management system built on PHP and MySQL.					
Execute Code; Bypass	11-04-2017	7.5	Unrestricted File Upload exists in BigTree CMS before 4.2.17: if an attacker uploads an 'xxx.php[space]' file, they could bypass a safety check and execute any code. **CVE ID: CVE-2017-7695**	NA	A-BIG-BIGTR-200417/29
Bluecoat					
Advanced Secure Gateway; Content Analysis System Software The web is one of the most common attack delivery mechanisms used by hackers to infect devices and infiltrate your network. With the Blue Coat Advanced Secure Gateway, you can shut down the web					

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

attack vector and enable users to safely use the web (cloud); The Content Analysis System (CAS) is Blue Coat's next-generation anti-virus, malware, and spyware management system.					
Execute Code	05-04-2017	9	Blue Coat Advanced Secure Gateway (ASG) 6.6 before 6.6.5.4 and Content Analysis System (CAS) 1.3 before 1.3.7.4 are susceptible to an OS command injection vulnerability. An authenticated malicious administrator can execute arbitrary OS commands with elevated system privileges. **CVE ID: CVE-2016-9091**	https://bto.bluecoat.com/security-advisory/sa138	A-BLU-ADVAN-200417/30
Botan Project					
Botan Botan is a BSD-licensed cryptographic library written in C++. It provides a wide variety of cryptographic algorithms, formats, and protocols, e.g. SSL and TLS.					
NA	10-04-2017	5	The X509_Certificate::allowed_usage function in botan 1.11.x before 1.11.31 might allow attackers to have unspecified impact by leveraging a call with more than one Key_Usage set in the enum value. **CVE ID: CVE-2016-6879**	https://botan.randombit.net/security.html#id2	A-BOT-BOTAN-200417/31
Gain Information	10-04-2017	5	botan 1.11.x before 1.11.22 makes it easier for remote attackers to decrypt TLS ciphertext data via a padding-oracle attack against TLS CBC ciphersuites. **CVE ID: CVE-2015-7824**	https://bugzilla.redhat.com/show_bug.cgi?id=1311613	A-BOT-BOTAN-200417/32
NA	10-04-2017	7.5	The Curve25519 code in botan before 1.11.31, on systems without a native 128-bit integer type, might allow attackers to have unspecified impact via vectors related to undefined behavior, as demonstrated on 32-bit ARM systems compiled by Clang. **CVE ID: CVE-2016-6878**	https://botan.randombit.net/security.html#id2	A-BOT-BOTAN-200417/33
NA	10-04-2017	7.5	botan 1.11.x before 1.11.22 improperly handles wildcard matching against hostnames,	https://botan.randombit.net/security.	A-BOT-BOTAN-200417/34

			which might allow remote attackers to have unspecified impact via a valid X.509 certificate, as demonstrated by accepting *.example.com as a match for bar.foo.example.com. **CVE ID: CVE-2015-7826**	html#id3	
DoS	10-04-2017	7.8	botan before 1.11.22 improperly validates certificate paths, which allows remote attackers to cause a denial of service (infinite loop and memory consumption) via a certificate with a loop in the certificate chain. **CVE ID: CVE-2015-7825**	https://bugzilla.redhat.com/show_bug.cgi?id=1311618	A-BOT-BOTAN-200417/35
Castle Rock Computing					
Snmpc SNMPc is a secure distributed network management system that will monitor your entire network infrastructure.					
XSS	09-04-2017	4.3	Castle Rock Computing SNMPc before 2015-12-17 has XSS via SNMP. **CVE ID: CVE-2015-6027**	https://community.rapid7.com/community/infosec/blog/2015/12/16/multiple-disclosures-for-multiple-network-management-systems	A-CAS-SNMPC-200417/36
Sql	09-04-2017	6.5	Castle Rock Computing SNMPc before 2015-12-17 has SQL injection via the sc parameter. **CVE ID: CVE-2015-6028**	https://community.rapid7.com/community/infosec/blog/2015/12/16/multiple-disclosures-for-multiple-network-management-systems	A-CAS-SNMPC-200417/37
Cisco					
Evolved Programmable Network Manager; Prime Infrastructure; Firepower Extensible Operating System;Unified Computing System; Firepower Management Center; Firepower Threat Defense; Mobility Services Engine; Prime Infrastructure; Registered Envelope Service; Unified Communications Manager; Unified Computing System; Unified Computing System Director; Wireless Lan Controller; Wireless Lan Controller 6.0; Wireless Lan Controller 7.0; Wireless Lan Controller 7.1 ; Wireless Lan Controller 7.2 ; Wireless Lan Controller 7.4 Cisco Systems, Inc. is American multinational technology conglomerate headquartered in San José, California, in the center of Silicon Valley, that develops, manufactures, and sells networking hardware, telecommunications equipment, and other high-technology services and products.					
Gain Information	07-04-2017	4	A vulnerability in the web interface of Cisco Prime	https://tools.cisco.com/se	A-CIS-EVOLV-

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

			Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to access sensitive data. The attacker does not need administrator credentials and could use this information to conduct additional reconnaissance attacks. More Information: CSCvc60031 (Fixed) CSCvc60041 (Fixed) CSCvc60095 (Open) CSCvc60102 (Open). Known Affected Releases: 2.2 2.2(3) 3.0 3.1(0.0) 3.1(0.128) 3.1(4.0) 3.1(5.0) 3.2(0.0) 2.0(4.0.45D). **CVE ID: CVE-2017-3884**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cpi	200417/38
NA	07-04-2017	3.6	A vulnerability in the CLI of Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb66189 CSCvb86775. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1742) 92.1(1.1658) 2.1(1.38) 2.0(1.107) 2.0(1.87) 1.1(4.148) 1.1(4.138). **CVE ID: CVE-2017-6602**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli2	A-CIS-FIREP-200417/39
NA	07-04-2017	3.6	A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli1	A-CIS-FIREP-200417/40

			Information: CSCvb61384 CSCvb86764. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1647). **CVE ID: CVE-2017-6601**		
NA	07-04-2017	7.2	A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61351 CSCvb61637. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1645) 2.0(1.82) 1.1(4.136. **CVE ID: CVE-2017-6600**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs1	A-CIS-FIREP-200417/41
Execute Code	07-04-2017	7.2	A vulnerability in the debug plug-in functionality of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to execute arbitrary commands, aka Privilege Escalation. More Information: CSCvb86725 CSCvb86797. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.105) 92.1(1.1733) 2.1(1.69). **CVE ID: CVE-2017-6598**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs	A-CIS-FIREP-200417/42
DoS	07-04-2017	7.1	A vulnerability in the detection engine reassembly of Secure Sockets Layer (SSL) packets for Cisco Firepower System Software could allow an unauthenticated, remote	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	A-CIS-FIREP-200417/43

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

			attacker to cause a denial of service (DoS) condition because the Snort process consumes a high level of CPU resources. Affected Products: This vulnerability affects Cisco Firepower System Software running software releases 6.0.0, 6.1.0, 6.2.0, or 6.2.1 when the device is configured with an SSL policy that has at least one rule specifying traffic decryption. More Information: CSCvc58563. Known Affected Releases: 6.0.0 6.1.0 6.2.0 6.2.1. **CVE ID: CVE-2017-3885**	sa-20170405-cfpw	
DoS Overflow	07-04-2017	4.3	A vulnerability in the detection engine that handles Secure Sockets Layer (SSL) packets for Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition because the Snort process unexpectedly restarts. This vulnerability affects Cisco Firepower System Software prior to the first fixed release when it is configured with an SSL Decrypt-Resign policy. More Information: CSCvb62292. Known Affected Releases: 6.0.1 6.1.0 6.2.0. Known Fixed Releases: 6.2.0 6.1.0.2. **CVE ID: CVE-2017-3887**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cfpw1	A-CIS-FIREP-200417/44
Gain Information	07-04-2017	7.2	A vulnerability in the CLI command parser of the Cisco Mobility Express 2800 and 3800 Series Wireless LAN Controllers could allow an authenticated, local attacker to obtain access to the underlying operating system shell with root-level privileges. More Information: CSCvb70351. Known Affected Releases:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cme	A-CIS-MOBIL-200417/45

			8.3(102.0). **CVE ID: CVE-2016-9197**		
XSS	07-04-2017	4.3	A vulnerability in the HTTP web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of the affected system. More Information: CSCuw63001 CSCuw63003. Known Affected Releases: 2.2(2). Known Fixed Releases: 3.1(0.0). **CVE ID: CVE-2017-3848**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170301-cpi	A-CIS-PRIME-200417/46
NA	07-04-2017	5.8	A vulnerability in the web interface of the Cisco Registered Envelope Service could allow an unauthenticated, remote attacker to redirect a user to a undesired web page, aka an Open Redirect. This vulnerability affects the Cisco Registered Envelope cloud-based service. More Information: CSCvc60123. Known Affected Releases: 5.1.0-015. **CVE ID: CVE-2017-3889**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-res	A-CIS-REGIS-200417/47
XSS	07-04-2017	3.5	A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability affects Cisco Unified Communications Manager with a default configuration running an affected software release with the attacker authenticated as the administrative user. More	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucm1	A-CIS-UNIFI-200417/48

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

			Information: CSCvc83712. Known Affected Releases: 12.0(0.98000.452). Known Fixed Releases:
			12.0(0.98000.750)
			12.0(0.98000.708)
			12.0(0.98000.707)
			12.0(0.98000.704)
			12.0(0.98000.554)
			12.0(0.98000.546)
			12.0(0.98000.543)
			12.0(0.98000.248)
			12.0(0.98000.244)
			12.0(0.98000.242).
			CVE ID: CVE-2017-3888		

Sql	07-04-2017	4	A vulnerability in the Cisco Unified Communications Manager web interface could allow an authenticated, remote attacker to impact the confidentiality of the system by executing arbitrary SQL queries, aka SQL Injection. The attacker must be authenticated as an administrative user to execute SQL database queries. More Information: CSCvc74291. Known Affected Releases:
			1.0(1.10000.10)
			11.5(1.10000.6). Known Fixed Releases: 12.0(0.98000.619)
			12.0(0.98000.485)
			12.0(0.98000.212)
			11.5(1.13035.1)
			11.0(1.23900.5)
			11.0(1.23900.2)
			11.0(1.23067.1)
			10.5(2.15900.2).
			CVE ID: CVE-2017-3886
				https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucm	A-CIS-UNIFI-200417/49

NA	07-04-2017	5.8	A vulnerability in the web interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability affects the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-	A-CIS-UNIFI-200417/50

			following Cisco products running Cisco IMC Software: Unified Computing System (UCS) B-Series M3 and M4 Blade Servers, Unified Computing System (UCS) C-Series M3 and M4 Rack Servers. More Information: CSCvc37931. Known Affected Releases: 3.1(2c)B. **CVE ID: CVE-2017-6604**	cimc	
NA	07-04-2017	4	A vulnerability in the role-based resource checking functionality of Cisco Unified Computing System (UCS) Director could allow an authenticated, remote attacker to view unauthorized information for any virtual machine in a UCS domain. More Information: CSCvc32434. Known Affected Releases: 5.5(0.1) 6.0(0.0). **CVE ID: CVE-2017-3817**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ucs-director	A-CIS-UNIFI-200417/51
DoS	07-04-2017	5	A vulnerability in RADIUS Change of Authorization (CoA) request processing in the Cisco Wireless LAN Controller (WLC) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition by disconnecting a single connection. This vulnerability affects Cisco Wireless LAN Controller running software release 8.3.102.0. More Information: CSCvb01835. Known Fixed Releases: 8.4(1.49) 8.3(111.0) 8.3(108.0) 8.3(104.24) 8.3(102.3). **CVE ID: CVE-2016-9195**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc1	A-CIS-WIREL-200417/52
DoS	06-04-2017	6.1	A vulnerability in 802.11 Wireless Multimedia Extensions (WME) action frame processing in Cisco Wireless LAN Controller (WLC) Software	https://tools.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-WIREL-200417/53

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 allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to incomplete input validation of the 802.11 WME packet header. An attacker could exploit this vulnerability by sending malformed 802.11 WME frames to a targeted device. A successful exploit could allow the attacker to cause the WLC to reload unexpectedly. The fixed versions are 8.0.140.0, 8.2.130.0, and 8.3.111.0. Cisco Bug IDs: CSCva86353. **CVE ID: CVE-2016-9194**	visory/cisco-sa-20170405-wlc	
Clip-bucket					
Clipbucket ClipBucket is an Open Source and freely downloadable PHP script that will let you start your own Video Sharing website (YouTube Clone) in a matter of minutes.					
XSS	06-04-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in ClipBucket 2.7.0.5 allow remote authenticated users to inject arbitrary web script or HTML via (1) the collection_description parameter to upload/manage_collections.php in an add_new action or the (2) photo_description, (3) photo_tags, or (4) photo_title parameter to upload/actions/photo_uploader.php. **CVE ID: CVE-2015-4673**	http://www.secpod.com/blog/clipbucket-2-7-0-5-multiple-stored-cross-site-scripting-vulnerability/	A-CLI-CLIPB-200417/54
XSS	06-04-2017	4.3	Multiple Cross Site Scripting (XSS) Vulnerabilities in ClipBucket v2.8.1 and probably prior allow Remote Attackers to inject arbitrary web script or HTML via (1) profile_desc, about_me, schools, occupation, companies, hobbies,	https://github.com/distributedweaknessfiling/DWF-Database-Artifacts/blob/master/DWF/2016/10	A-CLI-CLIPB-200417/55

			fav_movies, fav_music, fav_books parameters to ProfileSettings page; (2) note parameter to PersonalNotes Section; (3) closed_msg, description, allowed_types parameters to WebsiteConfigurations Section. NOTE: the collection_description vector is already covered by CVE-2015-4673. **CVE ID: CVE-2016-1000307**	00307/ CVE-2016-1000307.json	
Bosh Azure Cpi NA					
Execute Code	06-04-2017	4.6	Cloud Foundry Foundation BOSH Azure CPI v22 could potentially allow a maliciously crafted stemcell to execute arbitrary code on VMs created by the director, aka a "CPI code injection vulnerability." **CVE ID: CVE-2017-4964**	https://www.cloudfoundry.org/CVE-2017-4964/	A-CLO-BOSH-200417/56
Cloudera					
CDH CDH is Cloudera's 100% open source platform distribution, including Apache Hadoop and built specifically to meet enterprise demands					
Bypass	10-04-2017	5	Impala in CDH 5.2.0 through 5.7.2 and 5.8.0 allows remote attackers to bypass Setry authorization. **CVE ID: CVE-2016-6605**	https://www.cloudera.com/documentation/other/security-bulletins/topics/csb_all_product_issues.html#tsb_174	A-CLO-CDH-200417/57
Cloudviewnms					
Cloudview Nms CloudView is a standards-based network management system (NMS).					
XSS	09-04-2017	4.3	CloudView NMS before 2.10a has XSS via a TELNET login. **CVE ID: CVE-2016-5075**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multi	A-CLO-CLOUD-200417/58

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

				ple-disclosures-for-multiple-network-management-systems-part-2	
XSS	09-04-2017	4.3	CloudView NMS before 2.10a has XSS via SNMP. **CVE ID: CVE-2016-5073**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-CLO-CLOUD-200417/59
Gain Information	09-04-2017	5	CloudView NMS before 2.10a allows remote attackers to obtain sensitive information via a direct request for admin/auto.def. **CVE ID: CVE-2016-5076**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-CLO-CLOUD-200417/60
NA	09-04-2017	7.5	CloudView NMS before 2.10a has a format string issue exploitable over SNMP. **CVE ID: CVE-2016-5074**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-CLO-CLOUD-200417/61

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**										

Collectd					
Collectd Collectd is a Unix daemon that collects, transfers and stores performance data of computers and network equipment.					
DoS	03-04-2017	5	Incorrect interaction of the parse_packet() and parse_part_sign_sha256() functions in network.c in collectd 5.7.1 and earlier allows remote attackers to cause a denial of service (infinite loop) of a collectd instance (configured with "SecurityLevel None" and with empty "AuthFile" options) via a crafted UDP packet. **CVE ID: CVE-2017-7401**	https://github.com/collectd/collectd/issues/2174	A-COL-COLLE-200417/62
Deepin					
Deepin Desktop Environment DDE (Deepin Desktop Environment) is the default desktop environment originally created for the linux Deepin distribution.					
NA	10-04-2017	9	dde-daemon, the daemon process of DDE (Deepin Desktop Environment) 15.0 through 15.3, runs with root privileges and hardly does anything to identify the user who calls the function through D-Bus. Anybody can change the grub config, even to append some arguments to make a backdoor or privilege escalation, by calling DoWriteGrubSettings() provided by dde-daemon. **CVE ID: CVE-2017-7622**	https://github.com/kings-way/deepinhack/blob/master/dde_daemon_poc.py	A-DEE-DEEPI-200417/63
Digium					
Asterisk; Certified Asterisk Digium offers IP phones, business phone systems, such as Switchvox IP PBX, and custom communications solutions for Asterisk; Certified Asterisk is a branch of Asterisk supported by Digium for commercial, SLA customers, entitled under certain Support offerings.					
Execute Code Overflow	10-04-2017	6.5	Remote code execution can occur in Asterisk Open Source 13.x before 13.14.1 and 14.x before 14.3.1 and Certified Asterisk 13.13 before 13.13-	https://bugs.debian.org/859910	A-DIG-ASTER-200417/64

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

			cert3 because of a buffer overflow in a CDR user field, related to X-ClientCode in chan_sip, the CDR dialplan function, and the AMI Monitor action. **CVE ID: CVE-2017-7617**		
Djangoproject					
Django Django is a free and open-source web framework, written in Python, which follows the model-view-template (MVT) architectural pattern.					
NA	04-04-2017	5.8	A maliciously crafted URL to a Django (1.10 before 1.10.7, 1.9 before 1.9.13, and 1.8 before 1.8.18) site using the ``django.views.static.serve()`` view could redirect to any other domain, aka an open redirect vulnerability. **CVE ID: CVE-2017-7234**	https://www.djangoproject.com/weblog/2017/apr/04/security-releases/	A-DJA-DJANG-200417/65
XSS	04-04-2017	5.8	Django 1.10 before 1.10.7, 1.9 before 1.9.13, and 1.8 before 1.8.18 relies on user input in some cases to redirect the user to an "on success" URL. The security check for these redirects (namely ``django.utils.http.is_safe_url()``) considered some numeric URLs "safe" when they shouldn't be, aka an open redirect vulnerability. Also, if a developer relies on ``is_safe_url()`` to provide safe redirect targets and puts such a URL into a link, they could suffer from an XSS attack. **CVE ID: CVE-2017-7233**	https://www.djangoproject.com/weblog/2017/apr/04/security-releases/	A-DJA-DJANG-200417/66
Dropbox					
Lepton Lepton is a tool and file format for losslessly compressing JPEGs by an average of 22%.					
DoS	05-04-2017	4.3	The allocate_channel_framebuffer function in uncompressed_components.hh in Dropbox Lepton 1.2.1 allows	https://github.com/dropbox/lepton/commit/7789d99ac156adfd	A-DRO-LEPTO-200417/67

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

			remote attackers to cause a denial of service (divide-by-zero error and application crash) via a malformed JPEG image. **CVE ID: CVE-2017-7448**	7bbf66e7824bd3e948a74cf7	
Elfutils Project					
Elfutils Elfutils is a collection of various binary tools such as eu-objdump, eu-readelf, and other utilities that allow you to inspect and manipulate ELF files.					
DoS	09-04-2017	4.3	elflint.c in elfutils 0.168 does not validate the number of sections and the number of segments, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file. **CVE ID: CVE-2017-7613**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-memory-allocation-failure-in-xcalloc-xmalloc-c	A-ELF-ELFUT-200417/68
DoS Overflow	09-04-2017	4.3	The check_sysv_hash function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. **CVE ID: CVE-2017-7612**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-heap-based-buffer-overflow-in-check_sysv_hash-elflint-c	A-ELF-ELFUT-200417/69
DoS Overflow	09-04-2017	4.3	The check_symtab_shndx function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. **CVE ID: CVE-2017-7611**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-heap-based-buffer-overflow-in-check_symtab_shndx-elflint-c	A-ELF-ELFUT-200417/70
DoS Overflow	09-04-2017	4.3	The check_group function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. **CVE ID: CVE-2017-7610**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-heap-based-buffer-overflow-in-check_group-	A-ELF-ELFUT-200417/71

				elflint-c	
DoS	09-04-2017	4.3	elf_compress.c in elfutils 0.168 does not validate the zlib compression factor, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file. **CVE ID: CVE-2017-7609**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-memory-allocation-failure-in-__libelf_decompress-elf_compress-c	A-ELF-ELFUT-200417/72
DoS Overflow	09-04-2017	4.3	The ebl_object_note_type_name function in eblobjnotetypename.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. **CVE ID: CVE-2017-7608**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-heap-based-buffer-overflow-in-ebl_object_note_type_name-eblobjnotetypename-c	A-ELF-ELFUT-200417/73
DoS Overflow	09-04-2017	4.3	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file. **CVE ID: CVE-2017-7607**	https://blogs.gentoo.org/ago/2017/04/03/elfutils-heap-based-buffer-overflow-in-handle_gnu_hash-readelf-c	A-ELF-ELFUT-200417/74
Eparaksts					
Edoc-libraries;Eparakstitajs 3 With the arrival of eParaksts, information exchange with other state institutions and their representatives has become much faster, convenient and cheaper.					
Gain Information	09-04-2017	4.3	LVRTC eParakstitajs 3.0 (1.3.0) and edoc-libraries-2.5.4_01 allow attackers to read arbitrary files via crafted EDOC files. **CVE ID: CVE-2015-8276**	https://cert.lv/en/2016/01/new- CVE-information-avialable	A-EPA-EDOC--200417/75
NA	09-04-2017	4.3	LVRTC eParakstitajs 3.0 (1.3.0) and edoc-libraries-2.5.4_01 allow attackers to write to	https://cert.lv/en/2016/01/new- CVE-	A-EPA-EDOC--200417/76

			arbitrary files via crafted EDOC files. **CVE ID: CVE-2015-8275**	information-avialable	
Eyesofnetwork					
Eyesofnetwork EyesOfNetwork ("EON") is the OpenSource solution combining a pragmatic usage of ITIL processes and a technological interface allowing their workaday application.					
Execute Code Sql	11-04-2017	9	Multiple SQL injection vulnerabilities in EyesOfNetwork (aka EON) 5.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) bp_name, (2) display, (3) search, or (4) equipment parameter in module/monitoring_ged/ged_functions.php or the (5) type parameter in monitoring_ged/ajax.php. **CVE ID: CVE-2017-6088**	NA	A-EYE-EYESO-200417/77
F5					
Big-ip Access Policy Manager F5 BIG-IP Access Policy Manager (APM) is a flexible, high-performanceaccess and security solution that provides unified global access to your applications, network, and cloud.					
NA	11-04-2017	3.5	The TMM SSO plugin in F5 BIG-IP APM 12.0.0 - 12.1.1, 11.6.0 - 11.6.1 HF1, 11.5.4 - 11.5.4 HF2, when configured as a SAML Identity Provider with a Service Provider (SP) connector, might allow traffic to be disrupted or failover initiated when a malformed, signed SAML authentication request from an authenticated user is sent via the SP connector. **CVE ID: CVE-2016-7467**	https://support.f5.com/csp/article/K95444512	A-F5-BIG-I-200417/78
Ssl Intercept Iapp; Ssl Orchestrator NA					
Execute Code	06-04-2017	7.5	F5 SSL Intercept iApp version 1.5.0 - 1.5.7 is vulnerable to an unauthenticated, remote attack that may allow modification of the BIG-IP system configuration, extraction of	https://support.f5.com/csp/article/K53244431	A-F5-SSLI-200417/79

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

			sensitive system files, and possible remote command execution on the system when deployed using the Explicit Proxy feature plus SNAT Auto Map option for egress traffic. **CVE ID: CVE-2017-0305**		
Bypass	06-04-2017	5.8	F5 SSL Intercept iApp 1.5.0 - 1.5.7 and SSL Orchestrator 2.0 is vulnerable to a Server-Side Request Forgery (SSRF) attack when deployed using the Dynamic Domain Bypass (DDB) feature feature plus SNAT Auto Map option for egress traffic. **CVE ID: CVE-2017-6130**	https://support.f5.com/csp/article/K23001529	A-F5-SSL I-200417/80
Fiyo					
Fiyo Cms Fiyo CMS is one of hundreds Content Management System available on the internet.					
Execute Code	10-04-2017	7.5	In Fiyo CMS 2.x through 2.0.7, attackers may upload a webshell via the content parameter to "/dapur/apps/app_theme/libs/save_file.php" and then execute code. **CVE ID: CVE-2017-7625**	NA	A-FIY-FIYO -200417/81
Foxitsoftware					
Foxit Pdf Toolkit Foxit PDF Toolkit's suite of advanced modules provides high volume PDF creation and processing to optimize workflows.					
DoS; Execute Code; Overflow; Memory Corruption	07-04-2017	6.8	Memory Corruption Vulnerability in Foxit PDF Toolkit before 2.1 allows an attacker to cause Denial of Service & Remote Code Execution when a victim opens a specially crafted PDF file. **CVE ID: CVE-2017-7584**	https://www.foxitsoftware.com/support/security-bulletins.php	A-FOX-FOXIT-200417/82
Foxit Reader Foxit Reader is a lightweight, fast, and secure PDF Reader capable of high-volume processing. Download the best free PDF Reader today.					
Execute Code Overflow	04-04-2017	6.8	Heap-based buffer overflow in the CreateFXPDFConvertor function in ConvertToPdf_x86.dll in Foxit	NA	A-FOX-FOXIT-200417/83

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**										

			Reader 7.3.4.311 allows remote attackers to execute arbitrary code via a large SamplesPerPixel value in a crafted TIFF image that is mishandled during PDF conversion. This is fixed in 8.0. **CVE ID: CVE-2016-3740**		
Getpixie					
Pixie Pixie is a utility made especially for webmasters and designers.					
Execute Code	03-04-2017	7.5	Pixie 1.0.4 allows remote authenticated users to upload and execute arbitrary PHP code via the POST data in an admin/index.php?s=publish&x=filemanager request for a filename with a double extension, such as a .jpg.php file with Content-Type of image/jpeg. **CVE ID: CVE-2017-7402**	http://rungga.blogspot.co.id/2017/04/remote-file-upload-vulnerability-in.html	A-GET-PIXIE-200417/84
Getsymphony					
Symphony Cms Symphony is an XSLT-powered open source content management system.					
Execute Code	11-04-2017	6.5	Remote Code Execution vulnerability in symphony/content/content.blueprintsdatasources.php in Symphony CMS through 2.6.11 allows remote attackers to execute code and get a webshell from the back-end. The attacker must be authenticated and enter PHP code in the datasource editor or event editor. **CVE ID: CVE-2017-7694**	NA	A-GET-SYMPH-200417/85
GMV					
Checker Atm Security Checker ATM Security is the first software product designed specifically to protect ATMs from fraud.					
Execute Code	06-04-2017	9	GMV Checker ATM Security prior to 5.0.18 allows remote authenticated users to execute arbitrary code via unspecified vectors, aka PT-2017-03.	https://www.ptsecurity.com/ww-en/analytics/threatscape/	A-GMV-CHECK-200417/86

			CVE ID: CVE-2017-6968		
GNU					
Binutils The GNU Binary Utilities, or binutils, are a set of programming tools for creating and managing binary programs, object files, libraries, profile data, and assembly source code.					
DoS	09-04-2017	7.5	elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a "member access within null pointer" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an "int main() {return 0;}" program. **CVE ID: CVE-2017-7614**	https://blogs.gentoo.org/ago/2017/04/05/binutils-two-null-pointer-dereference-in-elflink-c/	A-GNU-BINUT-200417/87
Golang					
Crypto Package crypto collects common cryptographic constants.					
NA	04-04-2017	6.8	The Go SSH library (x/crypto/ssh) by default does not verify host keys, facilitating man-in-the-middle attacks. Default behavior changed in commit e4e2799 to require explicitly registering a hostkey verification mechanism. **CVE ID: CVE-2017-3204**	https://github.com/golang/go/issues/19767	A-GOL-CRYPT-200417/88
Google					
Chrome Google Chrome is a freeware web browser developed by Google.					
NA	11-04-2017	7.5	A use-after-free in AnimationController::endAnimationUpdate in Google Chrome. **CVE ID: CVE-2013-6647**	https://bugs.chromium.org/p/chromium/issues/detail?id=315889	A-GOO-CHROM-200417/89
Haxx					
Curl cURL is a computer software project providing a library and command-line tool for transferring data using various protocols.					
Gain Information	03-04-2017	2.1	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically	https://github.com/curl/curl/commit/	A-HAX-CURL-200417/90

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

		🟩	proximate attackers to obtain sensitive information from process memory in opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' character, which leads to a heap-based buffer over-read. **CVE ID: CVE-2017-7407**	1890d59905414ab84a35892b2e45833654aa5c13	
Helpdezk					
Helpdezk The HelpDEZk is a powerful management requests / incidents software.					
Execute Code; CSRF	05-04-2017	6.8	HelpDEZk 1.1.1 has CSRF in admin/home#/logos/ with an impact of remote execution of arbitrary PHP code. **CVE ID: CVE-2017-7447**	NA	A-HEL-HELPD-200417/91
CSRF	05-04-2017	6.8	HelpDEZk 1.1.1 has CSRF in admin/home#/person/ with an impact of obtaining admin privileges. **CVE ID: CVE-2017-7446**	NA	A-HEL-HELPD-200417/92
Horde					
Horde Groupware Horde Groupware is a free, enterprise ready, browser based collaboration suite.					
NA	04-04-2017	5.1	In Horde_Crypt before 2.7.6, as used in Horde Groupware Webmail Edition 5.x through 5.2.17, OS Command Injection can occur if the user has PGP features enabled in the user's preferences, and has enabled the "Should PGP signed messages be automatically verified when viewed?" preference. To exploit this vulnerability, an attacker can send a PGP signed email (that is maliciously crafted) to the Horde user, who then must either view or preview it. **CVE ID: CVE-2017-7414**	https://lists.horde.org/archives/horde/Week-of-Mon-20170403/056767.html	A-HOR-GROUP-200417/93
NA	04-04-2017	9	In Horde_Crypt before 2.7.6, as used in Horde Groupware Webmail Edition through	https://lists.horde.org/archives/horde	A-HOR-HORDE-200417/94

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

			5.2.17, OS Command Injection can occur if the attacker is an authenticated Horde Webmail user, has PGP features enabled in their preferences, and attempts to encrypt an email addressed to a maliciously crafted email address. **CVE ID: CVE-2017-7413**	/Week-of-Mon-20170403/056767.html	
Huawei					
Anyoffice; Espace Meeting; Fusionaccess; Fusionstorage; Hisuite; Logcenter; Utps Firmware Huawei Technologies Co. Ltd. is a Chinese multinational networking and telecommunications equipment and services company headquartered in Shenzhen, Guangdong.					
NA	02-04-2017	3.5	Huawei AnyOffice V200R006C00 could allow an authenticated, remote attacker to cause the software to deny services by uploading an XML bomb. **CVE ID: CVE-2016-8275**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160907-01-anyoffice-en	A-HUA-ANYOF-200417/95
NA	02-04-2017	6.6	In Huawei eSpace Meeting with software V100R001C03SPC201 and the earlier versions, attackers that obtain the permissions assigned to common users can elevate privileges to access and set specific key resources. **CVE ID: CVE-2014-3222**	http://www.huawei.com/en/psirt/security-advisories/hw-329170	A-HUA-ESPAC-200417/96
Gain Information	02-04-2017	4	Huawei FusionAccess with software V100R005C10 and V100R005C20 could allow remote attackers with specific permission to inject a Lightweight Directory Access Protocol (LDAP) operation command into a specific input variable to obtain sensitive information from the database. **CVE ID: CVE-2016-8779**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161130-01-ldap-en	A-HUA-FUSIO-200417/97
NA	02-04-2017	7.8	Huawei FusionAccess with software V100R005C10,V100R005C20 could allow attackers to craft	http://www.huawei.com/en/psirt/security-	A-HUA-FUSIO-200417/98

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 send a malformed HDP protocol packet to cause the virtual cloud desktop to be displaying an error and not usable. **CVE ID: CVE-2015-7844**	advisories/hw-453537	
NA	02-04-2017	4.1	The maintenance module in Huawei FusionStorage V100R003C30U1 allows attackers to create documents according to special rules to obtain the OS root privilege of FusionStorage. **CVE ID: CVE-2016-8803**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-01-fusionstorage-en	A-HUA-FUSIO-200417/99
Gain Information	02-04-2017	2.1	Huawei PC client software HiSuite 4.0.5.300_OVE has an information leak vulnerability; an attacker who can log in to the system can copy out the user's proxy password, causing information leaks. **CVE ID: CVE-2016-8272**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160905-01-hisuite-en	A-HUA-HISUI-200417/100
NA	02-04-2017	6.9	Huawei PC client software HiSuite 4.0.5.300_OVE uses insecure HTTP for upgrade software package download and does not check the integrity of the software package before installing; an attacker can launch an MITM attack to interrupt or replace the downloaded software package and further compromise the PC. **CVE ID: CVE-2016-8273**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160905-01-hisuite-en	A-HUA-HISUI-200417/101
Execute Code	02-04-2017	7.2	Huawei PC client software HiSuite 4.0.5.300_OVE has a dynamic link library (DLL) hijack vulnerability; an attacker can make the system load malicious DLL files to execute arbitrary code. **CVE ID: CVE-2016-8274**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160905-01-hisuite-en	A-HUA-HISUI-200417/102
DoS	02-04-2017	4	Huawei LogCenter V100R001C10 could allow an authenticated attacker to add	http://www.huawei.com/en/psirt/sec	A-HUA-LOGCE-200417/103

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

			abnormal device information to the log collection module, causing denial of service. **CVE ID: CVE-2015-8670**	urity-advisories/hw-464247	
NA	02-04-2017	6.5	Huawei LogCenter V100R001C10 could allow an authenticated attacker to tamper with requests using a tool and submit a request to the server for privilege escalation, affecting some system functions. **CVE ID: CVE-2015-8671**	http://www.huawei.com/en/psirt/security-advisories/hw-464243	A-HUA-LOGCE-200417/104
NA	02-04-2017	7.2	Huawei UTPS earlier than UTPS-V200R003B015D16SPC00C983 has an unquoted service path vulnerability which can lead to the truncation of UTPS service query paths. An attacker may put an executable file in the search path of the affected service and obtain elevated privileges after the executable file is executed. **CVE ID: CVE-2016-8769**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-utps-en	A-HUA-UTPS-200417/105
IBM					
Cognos Analytics IBM Cognos Analytics integrates reporting, modeling, analysis, dashboards, stories, metrics, and event management so you can understand your organization's data, and make effective business decisions.					
XSS	05-04-2017	3.5	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 Reference #: 1998887. **CVE ID: CVE-2016-3031**	http://www.ibm.com/support/docview.wss?uid=swg21998887	A-IBM-COGNO-200417/106
XSS	05-04-2017	3.5	IBM Cognos Analytics 11.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI	http://www.ibm.com/support/docview.wss?uid=swg21998887	A-IBM-COGNO-200417/107

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**										

			thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1998887. **CVE ID: CVE-2016-3015**		
Disposal And Governance Management For It;Global Retention Policy And Schedule Management IBM Global Retention Policy and Schedule Management is a single, cohesive retention management system. It provides natively integrated workflows and analytics to aid informationgovernance.					
CSRF	05-04-2017	6.8	IBM Disposal and Governance Management for IT and IBM Global Retention Policy and Schedule Management, components of IBM Atlas Policy Suite 6.0.3 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 Reference #: 2000771. **CVE ID: CVE-2016-6100**	http://www.ibm.com/support/docview.wss?uid=swg22000771	A-IBM-DISPO-200417/108
Tririga Application Platform IBM TRIRIGA Application Platform provides a single web-based set of design-time and runtime components.					
NA	05-04-2017	3.5	The IBM TRIRIGA Document Manager contains a vulnerability that could allow an authenticated user to execute actions they did not have access to. IBM Reference #: 2001084. **CVE ID: CVE-2017-1180**	http://www.ibm.com/support/docview.wss?uid=swg22001084	A-IBM-TRIRI-200417/109
Ilias Project					
Ilias ILIAS is an open source web-based learning management system (LMS).					
XSS	07-04-2017	4.3	ILIAS before 5.2.3 has XSS via SVG documents. **CVE ID: CVE-2017-7583**	https://github.com/ILIAS-eLearning/ILIAS/releases/tag/v5.2.3	A-ILI-ILIAS-200417/110
Imagemagick					
Imagemagick ImageMagick is a free and open-source software suite for displaying, converting, and editing raster					

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

image and vector image files.					
DoS	11-04-2017	2.1	The JPEG decoder in ImageMagick before 6.8.9-9 allows local users to cause a denial of service (out-of-bounds memory access and crash). **CVE ID: CVE-2014-8716**	https://bugzilla.redhat.com/show_bug.cgi?id=1164248	A-IMA-IMAGE-200417/111
DoS	05-04-2017	4.3	coders/sun.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted sun file. **CVE ID: CVE-2014-9829**	https://bugzilla.redhat.com/show_bug.cgi?id=1343485	A-IMA-IMAGE-200417/112
DoS	09-04-2017	4.3	coders/rle.c in ImageMagick 7.0.5-4 has an "outside the range of representable values of type unsigned char" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7606**	https://blogs.gentoo.org/ago/2017/04/02/imagemagick-undefined-behavior-in-codersrle-c/	A-IMA-IMAGE-200417/113
DoS	11-04-2017	4.3	coders/pnm.c in ImageMagick 6.9.0-1 Beta and earlier allows remote attackers to cause a denial of service (crash) via a crafted png file. **CVE ID: CVE-2014-9837**	https://anonscm.debian.org/cgit/collab-maint/imagemagick.git/commit/?h=debian-patches/6.8.9.9-4-for-upstream&id=7a7119c6fe19324ee17b8f756dae60c16e470ab2	A-IMA-IMAGE-200417/114
DoS	11-04-2017	4.3	DCM decode in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read). **CVE ID: CVE-2014-8562**	https://bugzilla.redhat.com/show_bug.cgi?id=1159362	A-IMA-IMAGE-200417/115
DoS	11-04-2017	4.3	PCX parser code in ImageMagick before 6.8.9-9	https://bugzilla.redhat.co	A-IMA-IMAGE-

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

			allows remote attackers to cause a denial of service (out-of-bounds read). **CVE ID: CVE-2014-8355**	m/show_bug.cgi?id=1158523	200417/116
DoS	11-04-2017	4.3	The HorizontalFilter function in resize.c in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file. **CVE ID: CVE-2014-8354**	https://bugzilla.redhat.com/show_bug.cgi?id=1158518	A-IMA-IMAGE-200417/117
NA	10-04-2017	5	In ImageMagick 7.0.4-9, an infinite loop can occur because of a floating-point rounding error in some of the color algorithms. This affects ModulateHSL, ModulateHCL, ModulateHCLp, ModulateHSB, ModulateHSI, ModulateHSV, ModulateHWB, ModulateLCHab, and ModulateLCHuv. **CVE ID: CVE-2017-7619**	https://www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=31506	A-IMA-IMAGE-200417/118
Imageworsener Project					
Imageworsener ImageWorsener is a cross-platform command-line utility and library for image scaling and other image processing.					
DoS; Overflow	05-04-2017	4.3	The iwgif_record_pixel function in imagew-gif.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file. **CVE ID: CVE-2017-7454**	https://github.com/jsummers/imageworsener/issues/11	A-IMA-IMAGE-200417/119
DoS	05-04-2017	4.3	The iwgif_record_pixel function in imagew-gif.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file. **CVE ID: CVE-2017-7453**	https://github.com/jsummers/imageworsener/issues/9	A-IMA-IMAGE-200417/120
DoS	05-04-2017	4.3	The iwbmp_read_info_header function in imagew-bmp.c in	https://github.com/jsum	A-IMA-IMAGE-

			libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted file. **CVE ID: CVE-2017-7452**	mers/imageworsener/issues/8	200417/121
NA	10-04-2017	4.3	The iw_read_bmp_file function in imagew-bmp.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to consume an amount of available memory via a crafted file. **CVE ID: CVE-2017-7624**	https://github.com/jsummers/imageworsener/issues/10	A-IMA-IMAGE-200417/122
DoS Overflow	10-04-2017	4.3	The iwmiffr_convert_row32 function in imagew-miff.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file. **CVE ID: CVE-2017-7623**	https://github.com/jsummers/imageworsener/issues/12	A-IMA-IMAGE-200417/123
Intel					
Hardware Accelerated Execution Manager Intel Hardware Accelerated Execution Manager (Intel HAXM) is a hardware-assisted virtualization engine (hypervisor) that uses Intel Virtualization Technology (Intel VT) to speed up Android* app emulation on a host machine.					
Gain Privileges	04-04-2017	7.2	Privilege escalation in IntelHAXM.sys driver in the Intel Hardware Accelerated Execution Manager before version 6.0.6 allows a local user to gain system level access. **CVE ID: CVE-2017-5683**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00072&languageid=en-fr	A-INT-HARDW-200417/124
Jive Software					
Jive Jive (formerly known as Clearspace, then Jive SBS, then Jive Engage) is a commercial Java EE-based Enterprise 2.0 collaboration and knowledge management tool produced by Jive Software.					
NA	09-04-2017	5.8	Jive before 2016.3.1 has an open redirect from the external-link.jspa page. **CVE ID: CVE-2016-4334**	http://www.ericgoldman.name/en/2016/vulnerability-report-jive-open-	A-JIV-JIVE-200417/125

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

				redirect/	
Keepassx Project					
Keepassx KeePassX is an application for people with extremly high demands on secure personal data management.					
Gain Information	10-04-2017	5	In KeePassX before 0.4.4, a cleartext copy of password data is created upon a cancel of an XML export action. This allows context-dependent attackers to obtain sensitive information by reading the .xml dotfile. **CVE ID: CVE-2015-8378**	http://bugs.debian.org/791858	A-KEE-KEEPA-200417/126
Kony					
Enterprise Mobile Management Enterprise Mobility Management (EMM) is the set of people, processes and technology focused on managing mobile devices, wireless networks, and other mobilecomputing services in a business context.					
Gain Information	11-04-2017	4	Kony Enterprise Mobile Management (EMM) before 4.2.5.2 has the vulnerability of disclosing the private key in clear-text when changing the parameters of the request. **CVE ID: CVE-2017-5672**	http://packetstormsecurity.com/files/142012/Kony-EMM-4.2.0-Private-Key-Disclosure.html	A-KON-ENTER-200417/127
Ladybird Web Solutions					
Faveo Helpdesk faveo-helpdesk - Faveo Open source ticketing system build on Laravel framework.					
CSRF	06-04-2017	6	public/rolechangeadmin in Faveo 1.9.3 allows CSRF. The impact is obtaining admin privileges. **CVE ID: CVE-2017-7571**	https://github.com/ladybirdweb/faveo-helpdesk/issues/446	A-LAD-FAVEO-200417/128
Lenovo					
Customer Care Software Development Kit NA					
Execute Code	10-04-2017	7.2	Privilege escalation in Lenovo Customer Care Software Development Kit (CCSDK) versions earlier than 2.0.16.3 allows local users to execute code with elevated privileges. **CVE ID: CVE-2016-8235**	https://support.lenovo.com/us/en/solutions/LEN-11340	A-LEN-CUSTO-200417/129
Updates					

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					
Execute Code	10-04-2017	9.3	Remote code execution in Lenovo Updates (not Lenovo System Update) allows man-in-the-middle attackers to execute arbitrary code. **CVE ID: CVE-2016-8237**	https://support.lenovo.com/us/en/solutions/LEN-8313	A-LEN-UPDAT-200417/130
Lg Project					
LG NA					
Gain Information	03-04-2017	5	lg.pl in Cistron-LG 1.01 stores sensitive information under the web root with insufficient access controls, which allows remote attackers to obtain IP addresses and other unspecified router credentials. **CVE ID: CVE-2014-3930**	NA	A-LG -LG-200417/131
Gain Information	03-04-2017	5	The default configuration for Cougar-LG stores sensitive information under the web root with insufficient access control, which might allow remote attackers to obtain private ssh keys. **CVE ID: CVE-2014-3929**	https://github.com/Cougar/lg/issues/5	A-LG -LG-200417/132
Gain Information	03-04-2017	5	Cougar-LG stores sensitive information under the web root with insufficient access control, which allows remote attackers to obtain credentials. **CVE ID: CVE-2014-3928**	https://github.com/Cougar/lg/issues/4	A-LG -LG-200417/133
Libaacplus Project					
Libaacplus Libaacplus is a shared version of the 3GPP reference implementation of High Efficiency Advanced Audio Codec (HE-AAC) Codec, also known as AAC+.					
DoS Overflow	09-04-2017	6.8	aacplusenc.c in HE-AAC+ Codec (aka libaacplus) 2.0.2 has an assertion failure, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted audio file. **CVE ID: CVE-2017-7605**	https://blogs.gentoo.org/ago/2017/04/01/libaacplus-signed-integer-overflow-left-shift-and-assertion-	A-LIB-LIBAA-200417/134

				failure/	
DoS	09-04-2017	6.8	au_channel.h in HE-AAC+ Codec (aka libaacplus) 2.0.2 has a left-shift undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted audio file. **CVE ID: CVE-2017-7604**	https://blogs.gentoo.org/ago/2017/04/01/libaacplus-signed-integer-overflow-left-shift-and-assertion-failure/	A-LIB-LIBAA-200417/135
DoS Overflow	09-04-2017	6.8	au_channel.h in HE-AAC+ Codec (aka libaacplus) 2.0.2 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted audio file. **CVE ID: CVE-2017-7603**	https://blogs.gentoo.org/ago/2017/04/01/libaacplus-signed-integer-overflow-left-shift-and-assertion-failure/	A-LIB-LIBAA-200417/136
Libarchive					
Libarchive Libarchive is a programming library that can create and read several different streaming archive formats, including most popular tar variants, several cpio formats, and both BSD and GNU ar variants. It can also write shar archives and read ISO9660 CDROM images and ZIP archives.					
DoS	03-04-2017	4.3	The archive_wstring_append_from_mbs function in archive_string.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted archive file. **CVE ID: CVE-2016-10209**	https://github.com/libarchive/libarchive/issues/842	A-LIB-LIBAR-200417/137
Libdwarf Project					
Libdwarf Libdwarf is a C library intended to simplify reading (and writing) applications using DWARF2, DWARF3.					
DoS	10-04-2017	5	dwarf_macro5.c in libdwarf before 20160923 allows remote attackers to cause a denial of service (NULL pointer dereference) via a debugging	https://www.prevanders.net/dwarfbug.html	A-LIB-LIBDW-200417/138

			information entry using DWARF5 and without a DW_AT_name. **CVE ID: CVE-2016-5041**		
Libming					
Libming A C library for generating SWF ("Flash") format movies. Ming includes a Python wrapper for the library.					
DoS; Overflow	07-04-2017	6.8	Multiple heap-based buffer overflows in parser.c in libming 0.4.7 allow remote attackers to cause a denial of service (listswf application crash) or possibly have unspecified other impact via a crafted SWF file. NOTE: this issue exists because of an incomplete fix for CVE-2016-9831. **CVE ID: CVE-2017-7578**	https://github.com/libming/libming/issues/68	A-LIB-LIBMI-200417/139
Libsamplerate Project					
Libsamplerate libsamplerate is a sample rate converter for audio.					
Overflow	11-04-2017	4.3	In libsamplerate before 0.1.9, a buffer over-read occurs in the calc_output_single function in src_sinc.c via a crafted audio file. **CVE ID: CVE-2017-7697**	https://github.com/erikd/libsamplerate/issues/11	A-LIB-LIBSA-200417/140
Libsndfile Project					
Libsndfile libsndfile is a widely used C library written by Erik de Castro Lopo for reading and writing audio files.					
Overflow	07-04-2017	4.3	In libsndfile before 1.0.28, an error in the "header_read()" function (common.c) when handling ID3 tags can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file. **CVE ID: CVE-2017-7586**	https://github.com/erikd/libsndfile/commit/f457b7b5ecfe91697ed01cfc825772c4d8de1236	A-LIB-LIBSN-200417/141
Overflow	07-04-2017	4.3	In libsndfile before 1.0.28, an error in the "flac_buffer_copy()" function (flac.c) can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file. **CVE ID: CVE-2017-7585**	http://www.mega-nerd.com/libsndfile/#History	A-LIB-LIBSN-200417/142

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

Libtiff					
Libtiff Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
DoS	09-04-2017	4.3	tif_dirread.c in LibTIFF 4.0.7 might allow remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image. **CVE ID: CVE-2017-7598**	NA	A-LIB-LIBTI-200417/143
DoS	09-04-2017	4.3	The JPEGSetupEncode function in tiff_jpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image. **CVE ID: CVE-2017-7595**	https://blogs.gentoo.org/ago/2017/04/01/libtiff-divide-by-zero-in-jpegsetupencode-tiff_jpeg-c	A-LIB-LIBTI-200417/144
DoS	09-04-2017	4.3	The OJPEGReadHeaderInfoSecTablesDcTable function in tif_ojpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (memory leak) via a crafted image. **CVE ID: CVE-2017-7594**	NA	A-LIB-LIBTI-200417/145
Overflow Gain Information	09-04-2017	4.3	tif_read.c in LibTIFF 4.0.7 does not ensure that tif_rawdata is properly initialized, which might allow remote attackers to obtain sensitive information from process memory via a crafted image. **CVE ID: CVE-2017-7593**	NA	A-LIB-LIBTI-200417/146
DoS Overflow	09-04-2017	6.8	LibTIFF 4.0.7 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7602**	NA	A-LIB-LIBTI-200417/147
DoS	09-04-2017	6.8	LibTIFF 4.0.7 has a "shift exponent too large for 64-bit type long" undefined behavior	NA	A-LIB-LIBTI-200417/148

			issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7601**		
DoS	09-04-2017	6.8	LibTIFF 4.0.7 has an "outside the range of representable values of type unsigned char" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7600**	https://blogs.gentoo.org/ago/2017/04/01/libtiff-multiple-ubsan-crashes	A-LIB-LIBTI-200417/149
DoS	09-04-2017	6.8	LibTIFF 4.0.7 has an "outside the range of representable values of type short" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7599**	NA	A-LIB-LIBTI-200417/150
DoS	09-04-2017	6.8	tif_dirread.c in LibTIFF 4.0.7 has an "outside the range of representable values of type float" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7597**	NA	A-LIB-LIBTI-200417/151
DoS	09-04-2017	6.8	LibTIFF 4.0.7 has an "outside the range of representable values of type float" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7596**	NA	A-LIB-LIBTI-200417/152

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

DoS	09-04-2017	6.8	The putagreytile function in tif_getimage.c in LibTIFF 4.0.7 has a left-shift undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image. **CVE ID: CVE-2017-7592**	NA	A-LIB-LIBTI-200417/153
Microsoft					
Edge Microsoft Edge is a web browser developed by Microsoft and included in Windows 10, Windows 10 Mobile and Xbox One, replacing Internet Explorer as the default web browser on all device classes.					
Execute Code; Overflow Memory Corruption	12-04-2017	7.6	A remote code execution vulnerability in Microsoft Edge exists in the way that the Scripting Engine renders when handling objects in memory in Microsoft browsers. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user, aka "Scripting Engine Memory Corruption Vulnerability." This CVE ID is unique from CVE-2017-0201. **CVE ID: CVE-2017-0093**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE ID: CVE-2017-0093	A-MIC-EDGE-200417/154
Mrlg4php Project					
Mrlg4php Multi-Router Looking Glass for PHP - a PHP repository on GitHub.					
Execute Code	03-04-2017	7.5	mrlg-lib.php in mrlg4php before 1.0.8 allows remote attackers to execute arbitrary shell code. **CVE ID: CVE-2014-3927**	https://github.com/infrastation/mrlg4php/issues/1	A-MRL-MRLG4-200417/155
Mybb					
Mybb MyBB is a free and open source PHP forum software.					
Bypass	06-04-2017	4	MyBB before 1.8.11 allows remote attackers to bypass an SSRF protection mechanism. **CVE ID: CVE-2017-7566**	https://blog.mybb.com/2017/04/04/mybb-1-8-11-merge-system-1-8-	A-MYB-MYBB-200417/156

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

				11-release/	
Netapp					
Clustered Data Ontap Clustered Data ONTAP provides up to 24 storage controllers or nodes managed as a single logical pool so your operations scale more easily.					
Gain Information	10-04-2017	5	NetApp OnCommand Performance Manager and OnCommand Unified Manager for Clustered Data ONTAP before 7.1P1 improperly bind the Java Management Extension Remote Method Invocation (aka JMX RMI) service to the network, which allows remote attackers to obtain sensitive information via unspecified vectors. **CVE ID: CVE-2017-7345**	https://kb.netapp.com/support/s/article/NTAP-20170331-0002	A-NET-CLUST-200417/157
DoS	10-04-2017	5	NetApp Clustered Data ONTAP 8.1 through 9.1P1, when NFS or SMB is enabled, allows remote attackers to cause a denial of service via unspecified vectors. **CVE ID: CVE-2017-5988**	https://kb.netapp.com/support/s/article/NTAP-20170331-0001	A-NET-CLUST-200417/158
Netikus					
Eventsentry EventSentry provides exceptional real time server monitoring, including server health, log file and event log monitoring at an affordable price.					
XSS	09-04-2017	4.3	Netikus EventSentry before 3.2.1.44 has XSS via SNMP. **CVE ID: CVE-2016-5077**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-NET-EVENT-200417/159
News System Project					
News System NA					
Execute Code; Sql	07-04-2017	7.5	SQL injection vulnerability in NewsController.php in the	https://www.ambionics.io	A-NEW-NEWS -

			News module 5.3.2 and earlier for TYPO3 allows unauthenticated users to execute arbitrary SQL commands via vectors involving overwriteDemand for order and OrderByAllowed. **CVE ID: CVE-2017-7581**	/blog/typo3-news-module-sqli	200417/160
Nextcloud					
Nextcloud Nextcloud 11 delivers a wide range of security and scalability improvements with a number of important features on top.					
Bypass	05-04-2017	4	Nextcloud Server before 9.0.55 and 10.0.2 suffers from a bypass in the quota limitation. Due to not properly sanitizing values provided by the `OC-Total-Length` HTTP header an authenticated adversary may be able to exceed their configured user quota. Thus using more space than allowed by the administrator. **CVE ID: CVE-2017-0887**	https://nextcloud.com/security/advisory/?id=nc-sa-2017-005	A-NEX-NEXTC-200417/161
DoS	05-04-2017	4	Nextcloud Server before 9.0.55 and 10.0.2 suffers from a Denial of Service attack. Due to an error in the application logic an authenticated adversary may trigger an endless recursion in the application leading to a potential Denial of Service. **CVE ID: CVE-2017-0886**	https://nextcloud.com/security/advisory/?id=nc-sa-2017-004	A-NEX-NEXTC-200417/162
Gain Information	05-04-2017	4	Nextcloud Server before 9.0.55 and 10.0.2 suffers from a error message disclosing existence of file in write-only share. Due to an error in the application logic an adversary with access to a write-only share may enumerate the names of existing files and subfolders by comparing the exception messages. **CVE ID: CVE-2017-0885**	https://nextcloud.com/security/advisory/?id=nc-sa-2017-003	A-NEX-NEXTC-200417/163
NA	05-04-2017	4	Nextcloud Server before 9.0.55	https://nextc	A-NEX-

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 10.0.2 suffers from a creation of folders in read-only folders despite lacking permissions issue. Due to a logical error in the file caching layer an authenticated adversary is able to create empty folders inside a shared folder. Note that this only affects folders and files that the adversary has at least read-only permissions for. **CVE ID: CVE-2017-0884**	loud.com/security/advisory/?id=nc-sa-2017-002	NEXTC-200417/164
NA	05-04-2017	4.3	Nextcloud Server before 9.0.55 and 10.0.2 suffers from a Content-Spoofing vulnerability in the "files" app. The top navigation bar displayed in the files list contained partially user-controllable input leading to a potential misrepresentation of information. **CVE ID: CVE-2017-0888**	https://nextcloud.com/security/advisory/?id=nc-sa-2017-006	A-NEX-NEXTC-200417/165
NA	05-04-2017	5.5	Nextcloud Server before 9.0.55 and 10.0.2 suffers from a permission increase on re-sharing via OCS API issue. A permission related issue within the OCS sharing API allowed an authenticated adversary to reshare shared files with an increasing permission set. This may allow an attacker to edit files in a share despite having only a 'read' permission set. Note that this only affects folders and files that the adversary has at least read-only permissions for. **CVE ID: CVE-2017-0883**	https://nextcloud.com/security/advisory/?id=nc-sa-2017-001	A-NEX-NEXTC-200417/166
Ninka Project					
Ninka Ninka is a lightweight license identification tool for source code.					
DoS; Gain Information	10-04-2017	7.5	Ninka before 1.3.2 might allow remote attackers to obtain	https://github.com/dmger	A-NIN-NINKA-

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

			sensitive information, manipulate license compliance scan results, or cause a denial of service (process hang) via a crafted filename. **CVE ID: CVE-2017-7239**	man/ninka/commit/81f185261c8863c5b84344ee31192870be939faf	200417/167
Objective Development					
Little Snitch Little Snitch offers a free, built-in demo mode that provides the same protection and functionality as the full version.					
NA	06-04-2017	4.6	Little Snitch version 3.0 through 3.7.3 suffer from a local privilege escalation vulnerability in the installer part. The vulnerability is related to the installation of the configuration file "at.obdev.littlesnitchd.plist" which gets installed to /Library/LaunchDaemons. **CVE ID: CVE-2017-2675**	https://www.obdev.at/products/littlesnitch/releasenotes.html	A-OBJ-LITTL-200417/168
Openbsd					
Openssh OpenSSH is the premier connectivity tool for remote login with the SSH protocol.					
NA	11-04-2017	7.5	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server. **CVE ID: CVE-2016-1908**	https://bugzilla.redhat.com/show_bug.cgi?id=1298741	A-OPE-OPENS-200417/169
Opencv					
Opencv OpenCV is released under a BSD license and hence it's free for both academic and commercial use.					
DoS	09-04-2017	4.3	OpenCV 3.0.0 allows remote attackers to cause a denial of service (segfault) via vectors involving corrupt chunks.	NA	A-OPE-OPENC-200417/170

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**										

			CVE ID: CVE-2016-1517		
Execute Code	09-04-2017	6.8	OpenCV 3.0.0 has a double free issue that allows attackers to execute arbitrary code. **CVE ID: CVE-2016-1516**	NA	A-OPE-OPENC-200417/171
Opendaylight					
Openflow OpenFlow is an open standard that enables researchers to run experimental protocols in the campus networks we use every day.					
NA	04-04-2017	5	OpenFlow plugin for OpenDaylight before Helium SR3 allows remote attackers to spoof the SDN topology and affect the flow of data, related to the reuse of LLDP packets, aka "LLDP Relay." **CVE ID: CVE-2015-1612**	https://cloudrouter.org/security/	A-OPE-OPENF-200417/172
NA	04-04-2017	5	OpenFlow plugin for OpenDaylight before Helium SR3 allows remote attackers to spoof the SDN topology and affect the flow of data, related to "fake LLDP injection." **CVE ID: CVE-2015-1611**	https://wiki.opendaylight.org/view/Security_Advisories#.5BModerate.5D_CVE-2015-1611_CVE-2015-1612_openflowplugin:_topology_spoofing_via_LLDP	A-OPE-OPENF-200417/173
Openidm Project					
Openidm OpenIDM is an identity management system written in the Java programming language.					
Gain Information	08-04-2017	4	In OpenIDM through 4.0.0 before 4.5.0, the info endpoint may leak sensitive information upon a request by the "anonymous" user, as demonstrated by responses with a 200 HTTP status code and a JSON object containing IP address strings. This is related to a missing access-control check in bin/defaults/script/info/login.js. **CVE ID: CVE-2017-7589**	https://backstage.forgerock.com/knowledge/kb/article/a92936505	A-OPE-OPENI-200417/174

XSS	08-04-2017	4.3	OpenIDM through 4.0.0 and 4.5.0 is vulnerable to reflected cross-site scripting (XSS) attacks within the Admin UI, as demonstrated by the _sortKeys parameter to the authzRoles script under managed/user/. **CVE ID: CVE-2017-7591**	https://backstage.forgerock.com/knowledge/kb/article/a92936505	A-OPE-OPENI-200417/175
XSS	08-04-2017	4.3	OpenIDM through 4.0.0 and 4.5.0 is vulnerable to persistent cross-site scripting (XSS) attacks within the Admin UI, as demonstrated by a crafted Managed Object Name. **CVE ID: CVE-2017-7590**	https://backstage.forgerock.com/knowledge/kb/article/a92936505	A-OPE-OPENI-200417/176
Openstack					
Horizon Horizon is the canonical implementation of OpenStack's Dashboard, which provides a web based user interface to OpenStack services including Nova, Swift, Keystone, etc.					
XSS	03-04-2017	3.5	OpenStack Horizon 9.x through 9.1.1, 10.x through 10.0.2, and 11.0.0 allows remote authenticated administrators to conduct XSS attacks via a crafted federation mapping. **CVE ID: CVE-2017-7400**	https://launchpad.net/bugs/1667086	A-OPE-HORIZ-200417/177
Opmantek					
Network Management Information System NMIS is an open source network management system that was first released in 1998.					
XSS	09-04-2017	3.5	Opmantek NMIS before 8.5.12G has XSS via SNMP. **CVE ID: CVE-2016-5642**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-OPM-NETWO-200417/178
NA	09-04-2017	6	Opmantek NMIS before 4.3.7c has command injection via man, finger, ping, trace, and nslookup in the tools.pl CGI	https://community.rapid7.com/community/infosec	A-OPM-NETWO-200417/179

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

			script. Versions before 8.5.12G might be affected in non-default configurations. **CVE ID: CVE-2016-6534**	/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	
Opsview					
Opsview Opsview is a software company specializing in enterprise systems monitoring software for physical, virtual, and cloud-based IT infrastructures.					
XSS	09-04-2017	4.3	Opsview before 2015-11-06 has XSS via SNMP. **CVE ID: CVE-2015-6035**	https://community.rapid7.com/community/infosec/blog/2015/12/16/multiple-disclosures-for-multiple-network-management-systems	A-OPS-OPSVI-200417/180
Osram					
Lightify Home Lightify Home is smart connected light for every home, simply controlled via App.					
NA	09-04-2017	5	OSRAM SYLVANIA Osram Lightify Home through 2016-07-26 allows Zigbee replay. **CVE ID: CVE-2016-5054**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/181
NA	09-04-2017	5	OSRAM SYLVANIA Osram	https://com	A-OSR-

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

			Lightify Home through 2016-07-26 does not use SSL pinning. **CVE ID: CVE-2016-5052**	munity.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities-CVE-2016-5051-through-5059	LIGHT-200417/182
Gain Information	09-04-2017	5	OSRAM SYLVANIA Osram Lightify Home before 2016-07-26 stores a PSK in cleartext under /private/var/mobile/Containers/Data/Application. **CVE ID: CVE-2016-5051**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/183
Execute Code	09-04-2017	7.5	OSRAM SYLVANIA Osram Lightify Home before 2016-07-26 allows remote attackers to execute arbitrary commands via TCP port 4000. **CVE ID: CVE-2016-5053**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-	A-OSR-LIGHT-200417/184

				5051-through-5059	
Lightify Pro OSRAM LIGHTIFY Pro solution - LIGHTIFY Pro is an intelligent, wireless lighting system configured via a tablet PC and controlled via mobile app.					
Gain Information	09-04-2017	4	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 allows attackers to obtain sensitive information by reading screenshots under /private/var/mobile/Containers/Data/Application. **CVE ID: CVE-2016-5059**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/185
XSS	09-04-2017	4.3	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 has XSS in the username field and Wireless Client Mode configuration page. **CVE ID: CVE-2016-5055**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/186
NA	09-04-2017	5	OSRAM SYLVANIA Osram Lightify Pro through 2016-07-26 allows Zigbee replay. **CVE ID: CVE-2016-5058**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-	A-OSR-LIGHT-200417/187

				multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	
NA	09-04-2017	5	OSRAM SYLVANIA Osram Lightify Pro through 2016-07-26 does not use SSL pinning. **CVE ID: CVE-2016-5057**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/188
NA	09-04-2017	5	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 uses only 8 hex digits for a PSK. **CVE ID: CVE-2016-5056**	https://community.rapid7.com/community/infosec/blog/2016/07/26/r7-2016-10-multiple-osram-sylvania-osram-lightify-vulnerabilities- CVE-2016-5051-through-5059	A-OSR-LIGHT-200417/189
Oxidforge					
Oxid Eshop					

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**										

With OXID eShop, online merchants or integration agencies get a lean, modern and feature rich PHP software to build up a sustainable e-commerce business.					
Execute Code	09-04-2017	6.5	OXID eShop before 2016-06-13 allows remote attackers to execute arbitrary code via a GET or POST request to the oxuser class. Fixed versions are Enterprise Edition v5.1.12, Enterprise Edition v5.2.9, Professional Edition v4.8.12, Professional Edition v4.9.9, Community Edition v4.8.12, Community Edition v4.9.9. **CVE ID: CVE-2016-5072**	https://oxidforge.org/en/security-bulletin-2016-001.html	A-OXI-OXID - 200417/190
Paessler					
Prtg Paessler Router Traffic Grapher, renamed PRTG Network Monitor from version 7 in 2008, is a server up-time and utilisation, network monitoring and bandwidth usage software package for server infrastructure from Paessler AG.					
XSS	09-04-2017	4.3	Paessler PRTG before 16.2.24.4045 has XSS via SNMP. **CVE ID: CVE-2016-5078**	https://community.rapid7.com/community/infosec/blog/2016/09/07/multiple-disclosures-for-multiple-network-management-systems-part-2	A-PAE-PRTG-200417/191
PHP					
PHP PHP (recursive acronym for PHP: Hypertext Preprocessor) is a widely-used open source general-purpose scripting language that is especially suited for web development and can be embedded into HTML.					
DoS	03-04-2017	5	** DISPUTED ** The _zval_get_long_func_ex in Zend/zend_operators.c in PHP 7.1.2 allows attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted use of "declare(ticks=" in a PHP script. NOTE: the vendor	NA	A-PHP-PHP-200417/192

			disputes the classification of this as a vulnerability, stating "Please do not request CVEs for ordinary bugs. CVEs are relevant for security issues only." **CVE ID: CVE-2017-6441**		
Phpmyfaq					
Phpmyfaq phpMyFAQ is a mobile-friendly, feature-rich, scalable open source FAQ software using PHP or HHVM.					
XSS	07-04-2017	4.3	inc/PMF/Faq.php in phpMyFAQ before 2.9.7 has XSS in the question field. **CVE ID: CVE-2017-7579**	http://www. phpmyfaq.de /security/ad visory-02-04-2017	A-PHP-PHPMY-200417/193
Pivotal Software					
Cloud Foundry; Cloud Foundry Elastic Runtime; Cloud Foundry Ops Manager; Cloud Foundry Uaa; Cloud Foundry Uaa Bosh Pivotal Software, Inc. (Pivotal) is a software and services company based in San Francisco and Palo Alto, California, with several other offices.					
Execute Code; Sql	11-04-2017	6.5	SQL injection vulnerability in Pivotal Cloud Foundry (PCF) before 238; UAA 2.x before 2.7.4.4, 3.x before 3.3.0.2, and 3.4.x before 3.4.1; UAA BOSH before 11.2 and 12.x before 12.2; Elastic Runtime before 1.6.29 and 1.7.x before 1.7.7; and Ops Manager 1.7.x before 1.7.8 allows remote authenticated users to execute arbitrary SQL commands via unspecified vectors. **CVE ID: CVE-2016-4468**	https://pivotal.io/security / CVE-2016-4468	A-PIV-CLOUD-200417/194
Pivotx					
Pivotx PivotX is an open source blog software written in PHP using either flat files or a database to store content.					
Execute Code	07-04-2017	6.5	PivotX 2.3.11 allows remote authenticated Advanced users to execute arbitrary PHP code by performing an upload with a safe file extension (such as .jpg) and then invoking the duplicate function to change to the .php extension.	https://gist.github.com/X1nda/749b6aac6e080624d9f8ec81321335df	A-PIV-PIVOT-200417/195

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 ID: CVE-2017-7570		
Podofo Project					
Podofo PoDoFo is a library to work with the PDF file format.					
DoS	03-04-2017	4.3	The PdfFontFactory.cpp:195:62 code in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PDF document. **CVE ID: CVE-2017-7383**	NA	A-POD-PODOF-200417/196
DoS	03-04-2017	4.3	The PdfFontFactory.cpp:200:88 code in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PDF document. **CVE ID: CVE-2017-7382**	NA	A-POD-PODOF-200417/197
DoS	03-04-2017	4.3	The doc/PdfPage.cpp:609:23 code in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PDF document. **CVE ID: CVE-2017-7381**	NA	A-POD-PODOF-200417/198
DoS	03-04-2017	4.3	The doc/PdfPage.cpp:614:20 code in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PDF document. **CVE ID: CVE-2017-7380**	NA	A-POD-PODOF-200417/199
DoS; Overflow	03-04-2017	4.3	The PoDoFo::PdfSimpleEncoding::ConvertToEncoding function in PdfEncoding.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a	NA	A-POD-PODOF-200417/200

			crafted PDF document. **CVE ID: CVE-2017-7379**		
DoS; Overflow	03-04-2017	4.3	The PoDoFo::PdfPainter::ExpandTabs function in PdfPainter.cpp in PoDoFo 0.9.5 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted PDF document. **CVE ID: CVE-2017-7378**	NA	A-POD-PODOF-200417/201
Proftpd					
Proftpd ProFTPD is an FTP server. ProFTPD is Free and open-source software, compatible with Unix-like systems and Microsoft Windows (via Cygwin).					
Bypass	04-04-2017	2.1	ProFTPD before 1.3.5e and 1.3.6 before 1.3.6rc5 controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks. Attackers with local access could bypass the AllowChrootSymlinks control by replacing a path component (other than the last one) with a symbolic link. The threat model includes an attacker who is not granted full filesystem access by a hosting provider, but can reconfigure the home directory of an FTP user. **CVE ID: CVE-2017-7418**	https://github.com/proftpd/proftpd/pull/444/commits/349addc3be4fcdad9bd4ec01ad1ccd916c898ed8	A-PRO-PROFT-200417/202
Proxygen Project					
Proxygen proxygen - A collection of C++ HTTP libraries including an easy to use HTTP server.					
Bypass	09-04-2017	5	Facebook Proxygen before 2015-11-09 mismanages HTTPMessage.request state, which allows remote attackers	https://groups.google.com/forum/#%21topic/fa	A-PRO-PROXY-200417/203

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 conduct hijacking attacks and bypass ACL checks. **CVE ID: CVE-2015-7265**	cebook-proxygen/K8wCXbW4ihs	
Bypass	09-04-2017	5	The SPDY/2 codec in Facebook Proxygen before 2015-11-09 allows remote attackers to conduct hijacking attacks and bypass ACL checks via a crafted host value. **CVE ID: CVE-2015-7263**	https://groups.google.com/forum/#%21topic/facebook-proxygen/K8wCXbW4ihs	A-PRO-PROXY-200417/204
NA	09-04-2017	7.5	The SPDY/2 codec in Facebook Proxygen before 2015-11-09 truncates a certain field to two bytes, which allows hijacking and injection attacks. **CVE ID: CVE-2015-7264**	https://groups.google.com/forum/#%21topic/facebook-proxygen/K8wCXbW4ihs	A-PRO-PROXY-200417/205
Pulp Project					
Pulp Pulp is a platform for managing repositories of software packages and making it available to a large numbers of consumers.					
NA	03-04-2017	5	Pulp before 2.3.0 uses the same the same certificate authority key and certificate for all installations. **CVE ID: CVE-2013-7450**	https://github.com/pulp/pulp/pull/627	A-PUL-PULP-200417/206
Qemu					
Qemu QEMU is a generic and open source machine emulator and virtualizer.					
Overflow	11-04-2017	1.9	Heap-based buffer overflow in QEMU, when built with the Q35-chipset-based PC system emulator. **CVE ID: CVE-2015-8666**	https://bugzilla.redhat.com/show_bug.cgi?id=1283722	A-QEM-QEMU-200417/207
DoS Overflow	11-04-2017	1.9	Stack-based buffer overflow in the megasas_ctrl_get_info function in QEMU, when built with SCSI MegaRAID SAS HBA emulation support, allows local guest users to cause a denial of service (QEMU instance crash) via a crafted SCSI controller CTRL_GET_INFO command. **CVE ID: CVE-2015-8613**	https://bugzilla.redhat.com/show_bug.cgi?id=1284008	A-QEM-QEMU-200417/208
DoS	10-04-2017	2.1	The (1) v9fs_create and (2) v9fs_lcreate functions in	https://bugzilla.redhat.co	A-QEM-QEMU-

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

			hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS privileged users to cause a denial of service (file descriptor or memory consumption) via vectors related to an already in-use fid. **CVE ID: CVE-2017-7377**	m/show_bug.cgi?id=1437871	200417/209
DoS	11-04-2017	3.5	Qemu, when built with VNC display driver support, allows remote attackers to cause a denial of service (arithmetic exception and application crash) via crafted SetPixelFormat messages from a client. **CVE ID: CVE-2015-8504**	http://git.qemu-project.org/?p=qemu.git;a=commitdiff;h=4c65fed8bdf96780735dbdb92a8	A-QEM-QEMU-200417/210
DoS Overflow	11-04-2017	4.7	Memory leak in QEMU, when built with a VMWARE VMXNET3 paravirtual NIC emulator support, allows local guest users to cause a denial of service (host memory consumption) by trying to activate the vmxnet3 device repeatedly. **CVE ID: CVE-2015-8568**	https://bugzilla.redhat.com/show_bug.cgi?id=1289816	A-QEM-QEMU-200417/211
Radare					
Radare2 Radare2 (also known as r2) is a complete framework for reverse-engineering and analyzing binaries, composed of a set of small utilities that can be used together or independently from the command line.					
DoS; Overflow	03-04-2017	6.8	The dalvik_disassemble function in libr/asm/p/asm_dalvik.c in radare2 1.2.1 allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted DEX file. **CVE ID: CVE-2017-6448**	https://github.com/radare/radare2/commit/f41e941341e44aa86edd4483c4487ec09a074257	A-RAD-RADAR-200417/212
DoS; Overflow	03-04-2017	6.8	The relocs function in libr/bin/p/bin_bflt.c in radare2 1.2.1 allows remote	https://github.com/radare/radare2/co	A-RAD-RADAR-200417/213

			attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted binary file. **CVE ID: CVE-2017-6194**	mmit/72794dc3523bbd5bb370de3c5857cb736c387e18	
Rogue Wave Software					
Jviews Rogue Wave helps organizations simplify complex software development, improve code quality, and shorten cycle times.					
Execute Code	06-04-2017	7.5	Rogue Wave JViews before 8.8 patch 21 and 8.9 before patch 1 allows remote attackers to execute arbitrary Java code that exists in the classpath, such as test code or administration code. The issue exists because the ilog.views.faces.IlvFacesController servlet in jviews-framework-all.jar does not require explicit configuration of servlets that can be called. **CVE ID: CVE-2015-8965**	https://rwkbp.makekb.com/?View=entry&EntryID=2521	A-ROG-JVIEW-200417/214
Ruby-lang					
Ruby Ruby is a dynamic, object-oriented programming language focused on simplicity and productivity.					
DoS	03-04-2017	5	The parse_char_class function in regparse.c in the Onigmo (aka Oniguruma-mod) regular expression library, as used in Ruby 2.4.0, allows remote attackers to cause a denial of service (deep recursion and application crash) via a crafted regular expression. **CVE ID: CVE-2017-6181**	https://bugs.ruby-lang.org/issues/13234	A-RUB-RUBY-200417/215
SAP					
Netweaver NetWeaver is an application builder from SAP for integrating business processes and databases from a number of sources while exploiting the leading Web services technologies.					
DoS	10-04-2017	4	The SAP EP-RUNTIME component in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to cause a	https://erpscan.com/advisories/erpscan-16-029-	A-SAP-NETWE-200417/216

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

			denial of service (out-of-memory error and service instability) via a crafted serialized Java object, as demonstrated by serial.cc3, aka SAP Security Note 2315788. **CVE ID: CVE-2016-10304**	sap-netweaver-java-7-5-deserialization-untrusted-user-value-trustmanagementservlet/	
Sql Anywhere SAP SQL Anywhere is a proprietary relational database management system (RDBMS) product from SAP.					
DoS Overflow	10-04-2017	4	Buffer overflow in the MobiLink Synchronization Server component in SAP SQL Anywhere 17 and possibly earlier allows remote authenticated users to cause a denial of service (resource consumption and process crash) by sending a crafted packet several times, aka SAP Security Note 2308778. **CVE ID: CVE-2016-10310**	NA	A-SAP-SQL A-200417/217
Trex Trex is a search engine in the SAP NetWeaver integrated technology platform produced by SAP AG using columnar storage.					
NA	11-04-2017	7.5	Code injection vulnerability exists in SAP TREX / Business Warehouse Accelerator (BWA). The vendor response is SAP Security Note 2419592. **CVE ID: CVE-2017-7691**	https://blogs.sap.com/2017/04/11/sap-security-patch-day-april-2017/	A-SAP-TREX-200417/218
Schneider-electric					
Interactive Graphical Scada System IGSS - Interactive Graphical SCADA System - is a state-of-the art SCADA system used for monitoring and controlling industrial processes.					
NA	07-04-2017	6.8	A DLL Hijacking issue was discovered in Schneider Electric Interactive Graphical SCADA System (IGSS) Software, Version 12 and previous versions. The software will execute a malicious file if it is named the same as a legitimate file and placed in a location that is	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2017-090-01	A-SCH-INTER-200417/219

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**										

			earlier in the search path. **CVE ID: CVE-2017-6033**		
Solarwinds					
Log & Event Manager Log & Event Manager normalizes logs so your rules and reports work regardless of the source.					
Gain Information	10-04-2017	4	SolarWinds Log & Event Manager (LEM) before 6.3.1 Hotfix 4 allows an authenticated user to browse the server's filesystem and read the contents of arbitrary files contained within. **CVE ID: CVE-2017-7646**	https://thwack.solarwinds.com/thread/111223	A-SOL-LOG &-200417/220
Execute Code	10-04-2017	6.5	SolarWinds Log & Event Manager (LEM) before 6.3.1 Hotfix 4 allows an authenticated user to execute arbitrary commands. **CVE ID: CVE-2017-7647**	https://thwack.solarwinds.com/thread/111223	A-SOL-LOG &-200417/221
Spiceworks					
Desktop Spiceworks is a professional network for the information technology industry that is headquartered in Austin, Texas					
XSS	09-04-2017	4.3	Spiceworks Desktop before 2015-12-01 has XSS via an SNMP response. **CVE ID: CVE-2015-6021**	https://community.rapid7.com/community/infosec/blog/2015/12/16/multiple-disclosures-for-multiple-network-management-systems	A-SPI-DESKT-200417/222
NA	06-04-2017	7.5	The Spiceworks TFTP Server, as distributed with Spiceworks Inventory 7.5, allows remote attackers to access the Spiceworks data\configurations directory by leveraging the unauthenticated nature of the TFTP service for all clients who can reach UDP port 69, as demonstrated by a WRQ (aka	NA	A-SPI-SPICE-200417/223

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**										

			Write request) operation for a configuration file or an executable file. **CVE ID: CVE-2017-7237**		
Splunk					
Hadoop Connect Splunk Hadoop Connect allows users to export data on disk.					
Execute Code Directory Traversal	06-04-2017	6.5	Splunk Hadoop Connect App has a path traversal vulnerability that allows remote authenticated users to execute arbitrary code, aka ERP-2041. **CVE ID: CVE-2017-7565**	https://www.splunk.com/view/SP-CAAAP2F	A-SPL-HADOO-200417/224
Splunk Splunk is an American multinational corporation based in San Francisco, California, that produces software for searching, monitoring, and analyzing machine-generated big data, via a web-style interface.					
Gain Information	10-04-2017	4.3	Splunk Enterprise 5.0.x before 5.0.18, 6.0.x before 6.0.14, 6.1.x before 6.1.13, 6.2.x before 6.2.13.1, 6.3.x before 6.3.10, 6.4.x before 6.4.6, and 6.5.x before 6.5.3 and Splunk Light before 6.5.2 assigns the $C JS property to the global Window namespace, which might allow remote attackers to obtain sensitive logged-in username and version-related information via a crafted webpage. **CVE ID: CVE-2017-5607**	https://www.splunk.com/view/SP-CAAAPZ3#InformationLeakageviaJavaScriptCVE20175607	A-SPL-SPLUN-200417/225
Starscream Project					
Starscream Project Starscream was a series of scientific experiments run by the Galactic Empire.					
Bypass	06-04-2017	5	WebSocket.swift in Starscream before 2.0.4 allows an SSL Pinning bypass because of incorrect management of the certValidated variable (it can be set to true but cannot be set to false). **CVE ID: CVE-2017-7192**	https://github.com/daltoniam/Starscream/commit/dbeb1190b8dcbff4f0b797f9e9d9b9b864d1f0d6	A-STA-STARS-200417/226
Bypass	06-04-2017	5	WebSocket.swift in Starscream before 2.0.4 allows an SSL	https://github.com/dalton	A-STA-STARS-

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**										

			Pinning bypass because pinning occurs in the stream function (this is too late; pinning should occur in the initStreamsWithData function). **CVE ID: CVE-2017-5887**	iam/Starscream/commit/dbeb1190b8dcbff4f0b797f9e9d9b9b864d1f0d6	200417/227
Swagger Project					
Swagger-ui Swagger UI is a dependency-free collection of HTML, Javascript, and CSS assets that dynamically generate beautiful documentation and sandbox from a Swagger-compliant API.					
XSS	09-04-2017	4.3	Swagger-UI before 2.2.1 has XSS via the Default field in the Definitions section. **CVE ID: CVE-2016-5682**	https://community.rapid7.com/community/infosec/blog/2016/09/02/r7-2016-19-persistent-xss-via-unescaped-parameters-in-swagger-ui	A-SWA-SWAGG-200417/228
Synology					
Photo Station Photo Station is a web service and application served by a Synology NAS.					
Execute Code	10-04-2017	6.5	Synology Photo Station before 6.3-2958 allows remote authenticated guest users to execute arbitrary commands via shell metacharacters in the X-Forwarded-For HTTP header to photo/login.php. **CVE ID: CVE-2016-10322**	NA	A-SYN-PHOTO-200417/229
Execute Code Gain Privileges	10-04-2017	7.2	Synology Photo Station before 6.3-2958 allows local users to gain privileges by leveraging setuid execution of a "synophoto_dsm_user --copy-no-ea" command. **CVE ID: CVE-2016-10323**	NA	A-SYN-PHOTO-200417/230
Textract Project					
Textract Textract supports a growing list of file types for text extraction.					
NA	06-04-2017	9.3	textract before 1.5.0 allows OS	http://seclist	A-TEX-

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

		🟥	Command Injection attacks via a filename in a call to the process function. This may be a remote attack if a web application accepts names of arbitrary uploaded files. **CVE ID: CVE-2016-10320**	s.org/oss-sec/2016/q4/442	TEXTR-200417/231
Trendmicro					
Interscan Web Security Virtual Appliance Trend Micro is the best global leaders in antivirus cloud computing security and internet content security software for PC& Mobile.					
XSS	05-04-2017	3.5	Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 before CP 1746 does not sanitize a rest/commonlog/report/template name field, which allows a 'Reports Only' user to inject malicious JavaScript while creating a new report. Additionally, IWSVA implements incorrect access control that allows any authenticated, remote user (even with low privileges like 'Auditor') to create or modify reports, and consequently take advantage of this XSS vulnerability. The JavaScript is executed when victims visit reports or auditlog pages. **CVE ID: CVE-2017-6340**	NA	A-TRE-INTER-200417/232
Interscan Web Security Virtual Appliance Trend Micro is the best global leaders in antivirus cloud computing security and internet content security software for PC& Mobile.					
NA	05-04-2017	4	Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 before CP 1746 mismanages certain key and certificate data. Per IWSVA documentation, by default, IWSVA acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to client browsers to complete a	NA	A-TRE-INTER-200417/233

			secure passage for HTTPS connections. It also allows administrators to upload their own certificates signed by a root CA. An attacker with low privileges can download the current CA certificate and Private Key (either the default ones or ones uploaded by administrators) and use those to decrypt HTTPS traffic, thus compromising confidentiality. Also, the default Private Key on this appliance is encrypted with a very weak passphrase. If an appliance uses the default Certificate and Private Key provided by Trend Micro, an attacker can simply download these and decrypt the Private Key using the default/weak passphrase. **CVE ID: CVE-2017-6339**		
NA	05-04-2017	4	Multiple Access Control issues in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 before CP 1746 allow an authenticated, remote user with low privileges like 'Reports Only' or 'Auditor' to change FTP Access Control Settings, create or modify reports, or upload an HTTPS Decryption Certificate and Private Key. **CVE ID: CVE-2017-6338**	NA	A-TRE-INTER-200417/234
Threat Discovery Appliance Trend Micro is the best global leaders in antivirus cloud computing security and internet content security software for PC& Mobile.					
Execute Code	12-04-2017	7.5	A command execution flaw on the Trend Micro Threat Discovery Appliance 2.6.1062r1 exists with the timezone parameter in the admin_sys_time.cgi interface. **CVE ID: CVE-2016-7547**	NA	A-TRE-THREA-200417/235

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**										

Directory Traversal Bypass	12-04-2017	10	On the Trend Micro Threat Discovery Appliance 2.6.1062r1, directory traversal when processing a session_id cookie allows a remote, unauthenticated attacker to delete arbitrary files as root. This can be used to bypass authentication or cause a DoS. **CVE ID: CVE-2016-7552**	NA	A-TRE-THREA-200417/236
Tryton					
Tryton Tryton. Is a three-tier high-level general purpose application platform under the license GPL-3 written in Python and using PostgreSQL as database engine.					
NA	04-04-2017	3.5	file_open in Tryton 3.x and 4.x through 4.2.2 allows remote authenticated users with certain permissions to read arbitrary files via a "same root name but with a suffix" attack. NOTE: This vulnerability exists because of an incomplete fix for CVE-2016-1242. **CVE ID: CVE-2017-0360**	http://hg.tryton.org/trytond?cmd=changeset;node=472510fdc6f8	A-TRY-TRYTO-200417/237
Unisys					
Secure Partitioning NA					
Gain Privileges	11-04-2017	4.6	Unquoted Windows search path vulnerability in the guest service in Unisys s-Par before 4.4.20 allows local users to gain privileges via a Trojan horse executable file in the %SYSTEMDRIVE% directory, as demonstrated by program.exe. **CVE ID: CVE-2017-5873**	http://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=41	A-UNI-SECUR-200417/238
Vbulletin					
Vbulletin vBulletin (vB) is a proprietary Internet forum software package developed by vBulletin Solutions, Inc., a division of Internet Brands.					
Bypass	06-04-2017	5	In vBulletin before 5.3.0, remote attackers can bypass the CVE-2016-6483 patch and conduct SSRF attacks by	https://www.vbulletin.com/forum/forum/vbulletin	A-VBU-VBULL-200417/239

			leveraging the behavior of the PHP parse_url function, aka VBV-17037. **CVE ID: CVE-2017-7569**	-announcements/vbulletin-announcements_aa/4367744-vbulletin-5-3-0-connect-is-now-available	
Veritas					
System Recovery With Veritas System Recovery, you can minimize downtime and avoid the impact of disaster by easily recovering in minutes, whether you're restoring a single file or email to an entire machine—physical or virtual.					
NA	05-04-2017	9.3	In Veritas System Recovery before 16 SP1, there is a DLL hijacking vulnerability in the patch installer if an attacker has write access to the directory from which the product is executed. **CVE ID: CVE-2017-7444**	https://www.veritas.com/content/support/en_US/security/VTS17-001.html#Issue1	A-VER-SYSTE-200417/240
Vertivco					
Liebert Multilink Automated Shutdown					
Gain Privileges	09-04-2017	7.2	Liebert MultiLink Automated Shutdown v4.2.4 allows local users to gain privileges by replacing the LiebertM executable file. **CVE ID: CVE-2015-7260**	https://stealthsploit.com/2015/10/27/vulnerability-disclosures/	A-VER-LIEBE-200417/241
Virustotal					
Yara YARA is an open source tool for identifying malware using a variety of techniques.					
DoS	03-04-2017	5	libyara/grammar.y in YARA 3.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted rule that is mishandled in the yr_compiler_destroy function. **CVE ID: CVE-2017-5924**	https://github.com/VirusTotal/yara/issues/593	A-VIR-YARA-200417/242
DoS	03-04-2017	5	libyara/grammar.y in YARA 3.5.0 allows remote attackers	https://github.com/Virus	A-VIR-YARA-200417/243

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 cause a denial of service (heap-based out-of-bounds read and application crash) via a crafted rule that is mishandled in the yara_yyparse function. **CVE ID: CVE-2017-5923**	Total/yara/commit/ab906da53ff2a68c6fd6d1fa73f2b7c7bf0bc636	
DoS	03-04-2017	5	libyara/grammar.y in YARA 3.5.0 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted rule that is mishandled in the yr_parser_lookup_loop_variable function. **CVE ID: CVE-2016-10211**	https://github.com/VirusTotal/yara/issues/575	A-VIR-YARA-200417/244
DoS	03-04-2017	5	libyara/lexer.l in YARA 3.5.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted rule that is mishandled in the yy_get_next_buffer function. **CVE ID: CVE-2016-10210**	https://github.com/VirusTotal/yara/issues/576	A-VIR-YARA-200417/245
Visioncritical					
Vision Critical Vision Critical's customer intelligence software enables companies to build engaged insight communities that offer real-time feedback.					
Gain Information	09-04-2017	5	Vision Critical before 2014-05-30 allows attackers to read arbitrary files via unspecified vectors, as demonstrated by image files and configuration files. **CVE ID: CVE-2014-2960**	https://www.visioncritical.com/customer-advisory-vision-critical-cto/	A-VIS-VISIO-200417/246
Web2py					
Web2py Web2py is an open source web application framework written in the Python programming language.					
NA	10-04-2017	5	web2py before 2.14.6 does not properly check if a host is denied before verifying passwords, allowing a remote attacker to perform brute-force attacks.	https://github.com/web2py/web2py/commit/944d8bd8f3c5cf8ae296fc03d	A-WEB-WEB2P-200417/247

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 ID: CVE-2016-10321	149056c65358426	
Websitebaker Project					
Websitebaker					
Execute Code; Sql	03-04-2017	7.5	Multiple SQL injection vulnerabilities in account/signup.php and account/signup2.php in WebsiteBaker 2.10.0 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) username, (2) display_name parameter. **CVE ID: CVE-2017-7410**	http://project.websitebaker.org/issues/39	A-WEB-WEBSI-200417/248
Wireshark					
Wireshark Wireshark is a network protocol analyzer for Unix and Windows.					
NA	12-04-2017	5	In Wireshark 2.2.0, the NCP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/CMakeLists.txt by registering this dissector. **CVE ID: CVE-2016-7958**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12945	A-WIR-WIRES-200417/249
NA	12-04-2017	5	In Wireshark 2.2.0, the Bluetooth L2CAP dissector could crash, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-btl2cap.c by avoiding use of a seven-byte memcmp for potentially shorter strings. **CVE ID: CVE-2016-7957**	https://bugs.wireshark.org/bugzilla/show_bug.cgi?id=12825	A-WIR-WIRES-200417/250
Wordpress					
Wordpress WordPress is a free and open-source content management system (CMS) based on PHP and MySQL.					
Na	02-04-2017	5	The register_routes function in wp-includes/rest-api/endpoints/class-wp-rest-posts-controller.php in the REST API in WordPress 4.7.x	https://github.com/WordPress/WordPress/commit/e357195ce3	A-WOR-WORDP-200417/251

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 4.7.2 does not require an integer identifier, which allows remote attackers to modify arbitrary pages via a request for wp-json/wp/v2/posts followed by a numeric value and a non-numeric value, as demonstrated by the wp-json/wp/v2/posts/123?id=123helloworld URI. **CVE ID: CVE-2017-1001000**	03017d517af f944644a7a1 232926f7	
Xiongmai Technologies					
Uc-httpd uc-httpd is an HTTP daemon used by a wide array of IoT devices					
Directory Traversal	07-04-2017	5	XiongMai uc-httpd has directory traversal allowing the reading of arbitrary files via a "GET ../" HTTP request. **CVE ID: CVE-2017-7577**	http://zeroday.insecurity.zone/exploits/uc-httpd_lfi.txt	A-XIO-UC-HT-200417/252
Xmlsoft					
Libxslt Libxslt is the XSLT C library developed for the GNOME project.					
NA	05-04-2017	5	In libxslt 1.1.29 and earlier, the EXSLT math.random function was not initialized with a random seed during startup, which could cause usage of this function to produce predictable outputs. **CVE ID: CVE-2015-9019**	NA	A-XML-LIBXS-200417/253
Yaml-cpp Project					
Yaml-cpp yaml-cpp is a YAML parser and emitter in C++.					
DoS Overflow	03-04-2017	4.3	The SingleDocParser::HandleNode function in yaml-cpp (aka LibYaml-C++) 0.5.3 allows remote attackers to cause a denial of service (stack consumption and application crash) via a crafted YAML file. **CVE ID: CVE-2017-5950**	NA	A-YAM-YAML--200417/254
Application ; Operating System (A / OS)					
Apple / Apple					
Apple Tv / Iphone Os ; Mac Os X ; Watchos ; Icloud ; Itunes ; Safari					

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

Apple is an American multinational technology company headquartered in Cupertino, California that designs, develops, and sells consumer electronics, computer software, and online services. Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch, iOS, macOS, watchOS and more.					
NA	01-04-2017	2.1	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves symlink mishandling in the "libarchive" component. It allows local users to change arbitrary directory permissions via unspecified vectors. **CVE ID: CVE-2017-2390**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/255
Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. The issue involves the "Keychain" component. It allows man-in-the-middle attackers to bypass an iCloud Keychain secret protection mechanism by leveraging lack of authentication for OTR packets. **CVE ID: CVE-2017-2448**	https://support.apple.com/HT207615	A-OS-APP-APPLE-200417/256
DoS	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreGraphics" component. It allows remote attackers to cause a denial of service (infinite recursion) via a crafted image. **CVE ID: CVE-2017-2417**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/257
DoS	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS	https://support.apple.com/HT20760	A-OS-APP-APPLE-200417/258

			before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to cause a denial of service (resource consumption) via a crafted text message. **CVE ID: CVE-2017-2461**	1	
DoS; Gain Information	01-04-2017	5.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted font file. **CVE ID: CVE-2017-2450**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/259
DoS; Gain Information	01-04-2017	5.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted font file. **CVE ID: CVE-2017-2439**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/260
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/261

			the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file. **CVE ID: CVE-2017-2487**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted file. **CVE ID: CVE-2017-2467**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/262
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Audio" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file. **CVE ID: CVE-2017-2462**	https://support.apple.com/HT207615	A-OS-APP-APPLE-200417/263
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreText" component. It allows remote attackers to	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/264

			execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file. **CVE ID: CVE-2017-2435**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted JPEG file. **CVE ID: CVE-2017-2432**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/265
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Audio" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted audio file. **CVE ID: CVE-2017-2430**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/266
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "ImageIO" component. It allows remote attackers to execute arbitrary code or cause a denial of service	https://support.apple.com/HT207602	A-OS-APP-APPLE-200417/267

			(memory corruption and application crash) via a crafted image file. **CVE ID: CVE-2017-2416**		
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code by leveraging an unspecified "type confusion." **CVE ID: CVE-2017-2415**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/268
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file. **CVE ID: CVE-2017-2407**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/269
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "FontParser" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted font file. **CVE ID: CVE-2017-2406**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/270

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

DoS Execute Code Overflow	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Carbon" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted .dfont file. **CVE ID: CVE-2017-2379**	https://support.apple.com/HT207615	A-OS-APP-APPLE-200417/271
NA	01-04-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves nghttp2 before 1.17.0 in the "HTTPProtocol" component. It allows remote HTTP/2 servers to have an unspecified impact via unknown vectors. **CVE ID: CVE-2017-2428**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/272
Execute Code	01-04-2017	7.6	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2478**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/273
Execute Code	01-04-2017	7.6	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/274

			affected. The issue involves the "Kernel" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2456**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2490**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/275
DoS Execute Code Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Security" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted X.509 certificate file. **CVE ID: CVE-2017-2485**	https://support.apple.com/HT207615	A-OS-APP-APPLE-200417/276
Execute Code Overflow	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/277

			via a crafted app. **CVE ID: CVE-2017-2483**		
Execute Code Overflow	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2482**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/278
Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. An off-by-one error allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2474**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/279
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2473**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/280
DoS Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected.	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/281

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

			watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app. **CVE ID: CVE-2017-2472**		
Execute Code Overflow	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Keyboards" component. A buffer overflow allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2458**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/282
DoS Execute Code Overflow	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Security" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (buffer overflow) via a crafted app. **CVE ID: CVE-2017-2451**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/283
Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "libc++abi" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code via a	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/284

			crafted C++ app that is mishandled during demangling. **CVE ID: CVE-2017-2441**		
DoS Execute Code Overflow	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (integer overflow) via a crafted app. **CVE ID: CVE-2017-2440**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/285
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2401**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/286
Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site. **CVE ID: CVE-2017-2479**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/287

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	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted use of frames on a web site. **CVE ID: CVE-2017-2475**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/288
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2476**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/289
XSS	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted frame objects. **CVE ID: CVE-2017-2445**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/290
Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site. **CVE ID: CVE-2017-2386**	https://support.apple.com/HT207600	A-OS-APP-APPLE-200417/291

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

Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site. **CVE ID: CVE-2017-2367**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/292
DoS Overflow Memory Corruption Gain Information	01-04-2017	5.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted web site. **CVE ID: CVE-2017-2447**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/293
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2481**	https://support.apple.com/HT207600	A-OS-APP-APPLE-200417/294
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/295

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 (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2470**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2469**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/296
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2468**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/297
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2466**	https://support.apple.com/HT207600	A-OS-APP-APPLE-200417/298
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/299

			before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2465**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2464**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/300
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2460**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/301
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/302

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 ID: CVE-2017-2459		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2455**	https://support.apple.com/HT207600	A-OS-APP-APPLE-200417/303
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2454**	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/304
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions. **CVE ID: CVE-2017-2446**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/305
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit"	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/306

			component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2396**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2395**	https://support.apple.com/HT207601	A-OS-APP-APPLE-200417/307
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2394**	https://support.apple.com/HT207600	A-OS-APP-APPLE-200417/308
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "CoreGraphics" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.	https://support.apple.com/HT207617	A-OS-APP-APPLE-200417/309

			CVE ID: CVE-2017-2444		
Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site. **CVE ID: CVE-2017-2480**	https://support.apple.com/HT207617	A-OS-APP-ICLOU-200417/310
NA	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to spoof the address bar via a crafted web site. **CVE ID: CVE-2017-2486**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/311
NA	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof FaceTime prompts in the user interface via a crafted web site. **CVE ID: CVE-2017-2453**	https://support.apple.com/HT207617	A-OS-APP-IPHON-200417/312
Bypass Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit JavaScript Bindings" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.	https://support.apple.com/HT207617	A-OS-APP-IPHON-200417/313

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 ID: CVE-2017-2442		
Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves mishandling of OpenGL shaders in the "WebKit" component. It allows remote attackers to obtain sensitive information from process memory via a crafted web site. **CVE ID: CVE-2017-2424**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/314
Bypass	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass a Content Security Policy protection mechanism via unspecified vectors. **CVE ID: CVE-2017-2419**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/315
DoS Overflow Memory Corruption	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows attackers to cause a denial of service (memory corruption and application crash) by leveraging a window-close action during a debugger-pause state. **CVE ID: CVE-2017-2377**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/316
NA	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar by leveraging text input during the loading of a page.	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/317

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 ID: CVE-2017-2376		
DoS	01-04-2017	5.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof an HTTP authentication sheet or cause a denial of service via a crafted web site. **CVE ID: CVE-2017-2389**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/318
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2433**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/319
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves bookmark creation in the "WebKit" component. It allows remote attackers to execute arbitrary code or spoof a bookmark by leveraging mishandling of links during drag-and-drop actions. **CVE ID: CVE-2017-2378**	https://support.apple.com/HT207617	A-OS-APP-IPHON-200417/320
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/321

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 application crash) via a crafted web site. **CVE ID: CVE-2017-2457**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2405**	https://support.apple.com/HT207600	A-OS-APP-IPHON-200417/322
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code via a crafted web site. **CVE ID: CVE-2017-2471**	https://support.apple.com/HT207617	A-OS-APP-IPHON-200417/323
DoS Execute Code Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. iCloud before 6.2 on Windows is affected. iTunes before 12.6 on Windows is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site. **CVE ID: CVE-2017-2463**	https://support.apple.com/HT207599	A-OS-APP-APPLE-200417/324
Canonical/Lightdm Project					
Ubuntu Linux/Lightdm					

Ubuntu is an open source software platform that runs everywhere from IoT devices, the smartphone, the tablet and the PC to the server and the cloud/LightDM is the display manager running in Ubuntu.					
Directory Traversal	05-04-2017	6.9	In LightDM through 1.22.0, a directory traversal issue in debian/guest-account.sh allows local attackers to own arbitrary directory path locations and escalate privileges to root when the guest user logs out. **CVE ID: CVE-2017-7358**	https://www.ubuntu.com/usn/usn-3255-1/	A-OS-CAN-UBUNT-200417/325
Cesanta/Cesanta					
Mongoose Embedded Web Server Library/Mongoose Os Cesanta are the specialists in embedded communications with products like Mongoose Embedded Web Server and Mongoose IoT Platform.					
DoS	10-04-2017	5	Use-after-free vulnerability in the mg_http_multipart_wait_for_boundary function in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.7 and earlier and Mongoose OS 1.2 and earlier allows remote attackers to cause a denial of service (crash) via a multipart/form-data POST request without a MIME boundary string. **CVE ID: CVE-2017-7185**	https://github.com/cesanta/mongoose/commit/b8402ed0733e3f244588b61ad5fedd093e3cf9cc	A-OS-CES-MONGO-200417/326
Cisco/Cisco					
Firepower Extensible Operating System/Unified Computing System					
NA	07-04-2017	7.2	A vulnerability in the local-mgmt CLI command of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61394 CSCvb86816. Known Affected Releases:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-cli	A-OS-CIS-FIREP-200417/327

			2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1658) 2.0(1.115). **CVE ID: CVE-2017-6597**		
Debian/Libtiff					
Debian Linux/Libtiff Debian is an operating system and a distribution of Free Software/ Libtiff is a library for reading and writing Tagged Image File Format (abbreviated TIFF) files.					
DoS	11-04-2017	4.3	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image. **CVE ID: CVE-2016-5322**	https://bugzilla.redhat.com/show_bug.cgi?id=1346694	A-OS-DEB-DEBIA-200417/328
Freeradius/Suse					
Freeradius/Linux Enterprise Server;Linux Enterprise Software Development Kit					
NA	05-04-2017	5	FreeRADIUS 2.2.x before 2.2.8 and 3.0.x before 3.0.9 does not properly check revocation of intermediate CA certificates. **CVE ID: CVE-2015-4680**	https://bugzilla.redhat.com/show_bug.cgi?id=1234975	A-OS-FRE-FREER-200417/329
Huawei/Huawei					
Fusionmanager/Usg2100 Firmware;Usg2200 Firmware;Usg5100 Firmware;Usg5500 Firmware;Usg9500 Firmware					
CSRF	02-04-2017	6.8	Huawei USG9500 with software V200R001C01SPC800 and earlier versions, V300R001C00; USG2100 with software V300R001C00SPC900 and earlier versions; USG2200 with software V300R001C00SPC900; USG5100 with software V300R001C00SPC900 could allow an unauthenticated, remote attacker to conduct a CSRF attack against the user of the web interface. **CVE ID: CVE-2014-9137**	http://www.huawei.com/en/psirt/security-advisories/hw-372186	A-OS-HUA-FUSIO-200417/330
CSRF	02-04-2017	6.8	Huawei FusionManager with software V100R002C03 and	http://www.huawei.com/en/psirt/sec	A-OS-HUA-FUSIO-200417/331

			V100R003C00 could allow an unauthenticated, remote attacker to conduct a CSRF attack against the user of the web interface. **CVE ID: CVE-2014-9136**	urity-advisories/hw-372186	
IBM;Util-linux Project/Redhat					
Power Hardware Management Console;Powerkvm/Util-linux/Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation					
DoS	11-04-2017	4.7	The parse_dos_extended function in partitions/dos.c in the libblkid library in util-linux allows physically proximate attackers to cause a denial of service (memory consumption) via a crafted MSDOS partition table with an extended partition boot record at zero offset. **CVE ID: CVE-2016-5011**	https://git.kernel.org/pub/scm/utils/util-linux/util-linux.git/commit/?id=7164a1c3	A-OS-IBM-POWER-200417/332
Redhat/Setroubleshoot Project					
Enterprise Linux Desktop;Enterprise Linux Hpc Node;Enterprise Linux Server;Enterprise Linux Workstation/Setroubleshoot					
Execute Code; Bypass	11-04-2017	6.9	setroubleshoot allows local users to bypass an intended container protection mechanism and execute arbitrary commands by (1) triggering an SELinux denial with a crafted file name, which is handled by the _set_tpath function in audit_data.py or via a crafted (2) local_id or (3) analysis_id field in a crafted XML document to the run_fix function in SetroubleshootFixit.py, related to the subprocess.check_output and commands.getstatusoutput functions, a different vulnerability than CVE ID: CVE-2016-4445.	https://github.com/fedora-selinux/setroubleshoot/commit/dda55aa50db95a25f0d919c3a0d5871827cdc40f	A-OS-RED-ENTER-200417/333

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 ID: CVE-2016-4989		
Execute Code	11-04-2017	6.9	The allow_execstack plugin for setroubleshoot allows local users to execute arbitrary commands by triggering an execstack SELinux denial with a crafted filename, related to the commands.getoutput function. **CVE ID: CVE-2016-4446**	https://github.com/fedora-selinux/setroubleshoot/commit/eaccf4c0d20a27d3df5ff6de8c9dcc80f6f40718	A-OS-RED-ENTER-200417/334
Execute Code	11-04-2017	6.9	The fix_lookup_id function in sealert in setroubleshoot before 3.2.23 allows local users to execute arbitrary commands as root by triggering an SELinux denial with a crafted file name, related to executing external commands with the commands.getstatusoutput function. **CVE ID: CVE-2016-4445**	https://bugzilla.redhat.com/show_bug.cgi?id=1339183	A-OS-RED-ENTER-200417/335
Execute Code	11-04-2017	6.9	The allow_execmod plugin for setroubleshoot before 3.2.23 allows local users to execute arbitrary commands by triggering an execmod SELinux denial with a crafted binary filename, related to the commands.getstatusoutput function. **CVE ID: CVE-2016-4444**	https://bugzilla.redhat.com/show_bug.cgi?id=1332644	A-OS-RED-ENTER-200417/336
Schneider-electric/Schneider-electric					
Modicon Tm221ce16r Firmware/Somachine					
NA	06-04-2017	7.5	Schneider Electric SoMachine Basic 1.4 SP1 and Schneider Electric Modicon TM221CE16R 1.3.3.3 devices have a hardcoded-key vulnerability. The Project Protection feature is used to prevent unauthorized users from opening an XML	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2017-097-01	A-OS-SCH-MODIC-200417/337

			protected project file, by prompting the user for a password. This XML file is AES-CBC encrypted; however, the key used for encryption (SoMachineBasicSoMachineBasicSoMa) cannot be changed. After decrypting the XML file with this key, the user password can be found in the decrypted data. After reading the user password, the project can be opened and modified with the Schneider product. **CVE ID: CVE-2017-7574**		
Hardware (H)					
Foscam					
C1;C1 Lite;C2;Fi9800xe;Fi9826p;Fi9828p;Fi9851p;Fi9853ep;Fi9901ep;Fi9903p;Fi9928p;R2					
NA	10-04-2017	4.3	Foscam networked devices use the same hardcoded SSL private key across different customers' installations, which allows remote attackers to defeat cryptographic protection mechanisms by leveraging knowledge of this key from another installation. **CVE ID: CVE-2017-7648**	http://www.securityfocus.com/archive/1/540388/30/0/threaded	H-FOS-C1;C1-200417/338
Gynoii					
Gcw-1010;Gcw-1020;Gpw-1025					
NA	09-04-2017	10	Gynoii has a password of guest for the backdoor guest account and a password of 12345 for the backdoor admin account. **CVE ID: CVE-2015-2881**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	H-GYN-GCW-1-200417/339

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

Philips					
In.sight B120\37					
XSS	09-04-2017	3.5	Philips In.Sight B120/37 has XSS, related to the Weaved cloud web service, as demonstrated by the name parameter to deviceSettings.php or shareDevice.php. **CVE ID: CVE-2015-2883**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	H-PHI-IN.SI-200417/340
Gain Information	09-04-2017	5	Philips In.Sight B120/37 allows remote attackers to obtain sensitive information via a direct request, related to yoics.net URLs, stream.m3u8 URIs, and cam_service_enable.cgi. **CVE ID: CVE-2015-2884**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	H-PHI-IN.SI-200417/341
NA	09-04-2017	10	Philips In.Sight B120/37 has a password of b120root for the backdoor root account, a password of /ADMIN/ for the backdoor admin account, a password of merlin for the backdoor mg3500 account, a password of M100-4674448 for the backdoor user account, and a password of M100-4674448 for the backdoor admin account. **CVE ID: CVE-2015-2882**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	H-PHI-IN.SI-200417/342
Samsung					
Galaxy S6 Samsung Galaxy S6 smartphone was launched in March 2015.					
NA	11-04-2017	6.8	SecEmailUI in Samsung Galaxy S6 does not sanitize HTML email content, allows	https://bugs.chromium.org/p/project-	H-SAM-GALAX-200417/343

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

			remote attackers to execute arbitrary JavaScript. **CVE ID: CVE-2015-7893**	zero/issues/detail?id=494&q=samsung&redir=1	
Trendnet					
Tv-ip743sic TRENDnet's Wi-Fi Baby Cam, model TV-IP743SIC, allows you to monitor your baby from any Internet connection.					
NA	09-04-2017	9	TRENDnet WiFi Baby Cam TV-IP743SIC has a password of admin for the backdoor root account. **CVE ID: CVE-2015-2880**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	H-TRE-TV-IP-200417/344
Operating System (OS)					
Airtame					
Hdmi Dongle Firmware					
NA	05-04-2017	10	AIRTAME HDMI dongle with firmware before 2.2.0 allows unauthenticated access to a big part of the management interface. It is possible to extract all information including the Wi-Fi password, reboot, or force a software update at an arbitrary time. **CVE ID: CVE-2017-7450**	http://cweiske.de/tagebuch/airtame-security.htm	O-AIR-HDMI-200417/345
Amazon					
Fire Os Amazon FireOS is an Android-based mobile operating system produced by Amazon for its FirePhone and Kindle Fire range of tablets, and other content delivery devices like Fire TV.					
DoS Overflow	09-04-2017	10	Stack-based buffer overflow in the havok_write function in drivers/staging/havok/havok.c in Amazon Fire OS before 2016-01-15 allows attackers to cause a denial of service (panic) or	https://marcograss.github.io/security/android/cve/2016/01/15/CVE ID: CVE-2015-7292-	O-AMA-FIRE-200417/346

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

			possibly have unspecified other impact via a long string to /dev/hv. **CVE ID: CVE-2015-7292**	amazon-kernel-stack-buffer-overflow.html	
Apple					
Iphone Os;Mac Os X; Mac Os Server Apple is an American multinational technology company headquartered in Cupertino, California that designs, develops, and sells consumer electronics, computer software, and online services.					
Gain Information	01-04-2017	2.1	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Siri" component. It allows physically proximate attackers to read text messages on the lock screen via unspecified vectors. **CVE ID: CVE-2017-2452**	https://support.apple.com/HT207617	O-APP-IPHON-200417/347
NA	01-04-2017	2.1	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Pasteboard" component. It allows physically proximate attackers to read the pasteboard by leveraging the use of an encryption key derived only from the hardware UID (rather than that UID in addition to the user passcode). **CVE ID: CVE-2017-2399**	https://support.apple.com/HT207617	O-APP-IPHON-200417/348
Gain Information	01-04-2017	2.1	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Accounts" component. It allows physically proximate attackers to discover an Apple ID by reading an iCloud authentication prompt on the lock screen. **CVE ID: CVE-2017-2397**	https://support.apple.com/HT207617	O-APP-IPHON-200417/349
Gain Information	01-04-2017	2.1	An issue was discovered in certain Apple products. iOS	https://support.apple.co	O-APP-IPHON-

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 10.3 is affected. The issue involves mishandling of deletion within the SQLite subsystem of the "Safari" component. It allows local users to identify the web-site visits that occurred in Private Browsing mode. **CVE ID: CVE-2017-2384**	m/HT207617	200417/350
NA	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "iTunes Store" component. It allows man-in-the-middle attackers to modify the client-server data stream to iTunes sandbox web services by leveraging use of cleartext HTTP. **CVE ID: CVE-2017-2412**	https://support.apple.com/HT207617	O-APP-IPHON-200417/351
XSS	01-04-2017	4.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Safari Reader" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site. **CVE ID: CVE-2017-2393**	https://support.apple.com/HT207617	O-APP-IPHON-200417/352
NA	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Phone" component. It allows attackers to trigger telephone calls to arbitrary numbers via a third-party app. **CVE ID: CVE-2017-2484**	https://support.apple.com/HT207617	O-APP-IPHON-200417/353
NA	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "DataAccess" component. It allows remote attackers to	https://support.apple.com/HT207617	O-APP-IPHON-200417/354

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

			access Exchange traffic in opportunistic circumstances by leveraging a mistake in typing an e-mail address. **CVE ID: CVE-2017-2414**		
NA	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "Quick Look" component. It allows remote attackers to trigger telephone calls to arbitrary numbers via a tel: URL in a PDF document, as exploited in the wild in October 2016. **CVE ID: CVE-2017-2404**	https://support.apple.com/HT207617	O-APP-IPHON-200417/355
Gain Information	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "SafariViewController" component. It allows attackers to obtain sensitive information by leveraging the SafariViewController's incorrect synchronization of Safari cache clearing. **CVE ID: CVE-2017-2400**	https://support.apple.com/HT207617	O-APP-IPHON-200417/356
Bypass	01-04-2017	5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the Simple Certificate Enrollment Protocol (SCEP) implementation in the the "Profiles" component. It allows remote attackers to bypass cryptographic protection mechanisms by leveraging DES support. **CVE ID: CVE-2017-2380**	https://support.apple.com/HT207617	O-APP-IPHON-200417/357
Overflow	05-04-2017	7.2	Wi-Fi in Apple iOS before 10.3.1 does not prevent CVE ID: CVE-2017-6956 stack buffer overflow exploitation via a crafted access point. NOTE: because an operating	https://support.apple.com/HT207688	O-APP-IPHON-200417/358

			system could potentially isolate itself from CVE-2017-6956 exploitation without patching Broadcom firmware functions, there is a separate CVE ID for the operating-system behavior. **CVE ID: CVE-2017-6975**		
NA	01-04-2017	10	An issue was discovered in certain Apple products. iOS before 10.3 is affected. The issue involves the "HomeKit" component. It allows attackers to have an unspecified impact by leveraging the presence of Home Control on Control Center. **CVE ID: CVE-2017-2434**	https://support.apple.com/HT207617	O-APP-IPHON-200417/359
Bypass	01-04-2017	7.5	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. The issue involves the "Security" component. It allows remote attackers to bypass intended access restrictions by leveraging a successful result from a SecKeyRawVerify API call with an empty signature. **CVE ID: CVE-2017-2423**	https://support.apple.com/HT207615	O-APP-IPHON-200417/360
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. iOS before 10.3 is affected. macOS before 10.12.4 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2398**	https://support.apple.com/HT207617	O-APP-IPHON-200417/361
Gain Information	01-04-2017	5	An issue was discovered in certain Apple products.	https://support.apple.co	O-APP-MAC O-

			macOS Server before 5.3 is affected. The issue involves the "Wiki Server" component. It allows remote attackers to enumerate user accounts via unspecified vectors. **CVE ID: CVE-2017-2382**	m/HT207604	200417/362
Gain Information	01-04-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Hypervisor" component. It allows guest OS users to obtain sensitive information from the CR8 control register via unspecified vectors. **CVE ID: CVE-2017-2418**	https://support.apple.com/HT207615	O-APP-MAC O-200417/363
NA	01-04-2017	2.1	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves mishandling of DMA in the "EFI" component. It allows physically proximate attackers to discover the FileVault 2 encryption password via a crafted Thunderbolt adapter. **CVE ID: CVE-2016-7585**	https://support.apple.com/HT207615	O-APP-MAC O-200417/364
NA	01-04-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the system-installation subsystem of the "System Integrity Protection" component. It allows attackers to modify the contents of a protected disk location via a crafted app. **CVE ID: CVE-2017-6974**	https://support.apple.com/HT207615	O-APP-MAC O-200417/365
Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves	https://support.apple.com/HT207615	O-APP-MAC O-200417/366

			the "Intel Graphics Driver" component. It allows attackers to obtain sensitive information from kernel memory via a crafted app. **CVE ID: CVE-2017-2489**		
Gain Information	01-04-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "iBooks" component. It allows remote attackers to obtain sensitive information from local files via a file: URL in an iBooks file. **CVE ID: CVE-2017-2426**	https://support.apple.com/HT207615	O-APP-MAC O-200417/367
DoS	01-04-2017	4.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireFamily" component. It allows attackers to cause a denial of service (NULL pointer dereference) via a crafted app. **CVE ID: CVE-2017-2388**	https://support.apple.com/HT207615	O-APP-MAC O-200417/368
Bypass	01-04-2017	5	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "FinderKit" component. It allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging unexpected permission changes during an iCloud Sharing Send Link action. **CVE ID: CVE-2017-2429**	https://support.apple.com/HT207615	O-APP-MAC O-200417/369
DoS; Gain Information	01-04-2017	5.8	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Menus" component. It allows attackers to obtain sensitive information or	https://support.apple.com/HT207615	O-APP-MAC O-200417/370

			cause a denial of service (out-of-bounds read and application crash) via a crafted app. **CVE ID: CVE-2017-2409**		
Gain Privileges	01-04-2017	6.5	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "sudo" component. It allows remote authenticated users to gain privileges by leveraging membership in the admin group on a network directory server. **CVE ID: CVE-2017-2381**	https://support.apple.com/HT207615	O-APP-MACO-200417/371
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "CoreMedia" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted .mov file. **CVE ID: CVE-2017-2431**	https://support.apple.com/HT207615	O-APP-MACO-200417/372
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "SecurityFoundation" component. A double free vulnerability allows remote attackers to execute arbitrary code via a crafted certificate. **CVE ID: CVE-2017-2425**	https://support.apple.com/HT207615	O-APP-MACO-200417/373
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "QuickTime" component. It allows remote attackers to execute arbitrary code or cause a	https://support.apple.com/HT207615	O-APP-MACO-200417/374

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

			denial of service (memory corruption and application crash) via a crafted media file. **CVE ID: CVE-2017-2413**		
Execute Code	01-04-2017	6.8	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Printing" component. A format-string vulnerability allows remote attackers to execute arbitrary code via a crafted ipp: or ipps: URL. **CVE ID: CVE-2017-2403**	https://support.apple.com/HT207615	O-APP-MACO-200417/375
DoS; Overflow; Gain Privileges; Memory Corruption	01-04-2017	7.2	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOFireWireAVC" component. It allows local users to gain privileges or cause a denial of service (memory corruption) via unspecified vectors. **CVE ID: CVE-2017-2437**	https://support.apple.com/HT207615	O-APP-MACO-200417/376
DoS; Overflow; Memory Corruption	01-04-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "libxslt" component. It allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors. **CVE ID: CVE-2017-2477**	https://support.apple.com/HT207615	O-APP-MACO-200417/377
Bypass	01-04-2017	7.5	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves mishandling of profile uninstall actions in the "MCX Client" component when a profile has multiple payloads. It allows remote	https://support.apple.com/HT207615	O-APP-MACO-200417/378

			attackers to bypass intended access restrictions by leveraging Active Directory certificate trust that should not have remained. **CVE ID: CVE-2017-2402**		
DoS Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app. **CVE ID: CVE-2017-2449**	https://support.apple.com/HT207615	O-APP-MACO-200417/379
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Intel Graphics Driver" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2443**	https://support.apple.com/HT207615	O-APP-MACO-200417/380
DoS Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleRAID" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (use-after-free) via a crafted app. **CVE ID: CVE-2017-2438**	https://support.apple.com/HT207615	O-APP-MACO-200417/381
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves	https://support.apple.com/HT207615	O-APP-MACO-200417/382

			the "IOFireWireAVC" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2436**		
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2427**	https://support.apple.com/HT207615	O-APP-MACO-200417/383
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Multi-Touch" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2422**	https://support.apple.com/HT207615	O-APP-MACO-200417/384
Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "AppleGraphicsPowerManagement" component. A race condition allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2421**	https://support.apple.com/HT207615	O-APP-MACO-200417/385

DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Bluetooth" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2420**	https://support.apple.com/HT207615	O-APP-MACO-200417/386
Execute Code	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "Kernel" component. It allows attackers to execute arbitrary code in a privileged context via a crafted app. **CVE ID: CVE-2017-2410**	https://support.apple.com/HT207615	O-APP-MACO-200417/387
DoS; Execute Code; Overflow; Memory Corruption	01-04-2017	9.3	An issue was discovered in certain Apple products. macOS before 10.12.4 is affected. The issue involves the "IOATAFamily" component. It allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2017-2408**	https://support.apple.com/HT207615	O-APP-MACO-200417/388
Arm Trusted Firmware Project					
Arm Trusted Firmware					
Execute Code; Overflow	06-04-2017	4.3	In ARM Trusted Firmware 1.2 and 1.3, a malformed firmware update SMC can result in copying unexpectedly large data into secure memory because of integer overflows. This affects certain cases involving execution of both	https://github.com/ARM-software/arm-trusted-firmware/wiki/ARM-Trusted-Firmware-Security-	O-ARM-ARMT-200417/389

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**										

			AArch64 Generic Trusted Firmware (TF) BL1 code and other firmware update code. **CVE ID: CVE-2016-10319**	Advisory-TFV-1	
Axis					
Axis Communications Firmware Axis specializes in professional network video and printing solutions.					
CSRF	09-04-2017	6.8	AXIS Communications products allow CSRF, as demonstrated by admin/pwdgrp.cgi, vaconfig.cgi, and admin/local_del.cgi. **CVE ID: CVE-2015-8255**	https://www.exploit-db.com/exploits/41626/	O-AXI-AXIS - 200417/390
NA	09-04-2017	7.8	AXIS Communications products with firmware through 5.80.x allow remote attackers to modify arbitrary files as root via vectors involving Open Script Editor, aka a "resource injection vulnerability." **CVE ID: CVE-2015-8258**	https://www.exploit-db.com/exploits/41625/	O-AXI-AXIS - 200417/391
Backbox					
Backbox Linux BackBox is a penetration test and security assessment oriented Ubuntu-based Linux distribution providing a network and informatic systems analysis toolkit.					
DoS	03-04-2017	5	** DISPUTED ** BackBox Linux 4.6 allows remote attackers to cause a denial of service (ksoftirqd CPU consumption) via a flood of packets with Martian source IP addresses (as defined in RFC 1812 section 5.3.7). This product enables net.ipv4.conf.all.log_martians by default. NOTE: the vendor reports "It has been proved that this vulnerability has no foundation and it is totally fake and based on false assumptions."	NA	O-BAC-BACKB-200417/392

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 ID: CVE-2017-7397		
Bluecoat					
Ssl Visibility Appliance Sv1800 Firmware;Ssl Visibility Appliance Sv2800 Firmware;Ssl Visibility Appliance Sv3800 Firmware;Ssl Visibility Appliance Sv800 Firmware NA					
NA	11-04-2017	4.3	Blue Coat SSL Visibility (SSLV) 3.x before 3.11.3.1 is susceptible to a denial-of-service vulnerability that impacts the SSL servers for intercepted SSL connections. A malicious SSL client can, under certain circumstances, temporarily exhaust the TCP connection pool of an SSL server. **CVE ID: CVE-2016-10259**	https://bto.bluecoat.com/security-advisory/sa142	O-BLU-SSL V-200417/393
Broadcom					
Hardmac Wi-fi Soc Firmware NA					
Execute Code Overflow	05-04-2017	8.3	On the Broadcom Wi-Fi HardMAC SoC with fbt firmware, a stack buffer overflow occurs when handling an 802.11r (FT) authentication response, leading to remote code execution via a crafted access point that sends a long R0KH-ID field in a Fast BSS Transition Information Element (FT-IE). **CVE ID: CVE-2017-6956**	NA	O-BRO-HARDM-200417/394
Brother					
Ads Firmware;Dcp Firmware;Hl Firmware;Mfc Firmware NA					
NA	12-04-2017	10	On certain Brother devices, authorization is mishandled by including a valid AuthCookie cookie in the HTTP response to a failed login attempt. Affected models are: MFC-J6973CDW MFC-J4420DW MFC-8710DW MFC-J4620DW MFC-L8850CDW MFC-J3720	https://cxsecurity.com/blad/WLB-2017040064	O-BRO-ADS F-200417/395

			MFC-J6520DW MFC-L2740DW MFC-J5910DW MFC-J6920DW MFC-L2700DW MFC-9130CW MFC-9330CDW MFC-9340CDW MFC-J5620DW MFC-J6720DW MFC-L8600CDW MFC-L9550CDW MFC-L2720DW DCP-L2540DW DCP-L2520DW HL-3140CW HL-3170CDW HL-3180CDW HL-L8350CDW HL-L2380DW ADS-2500W ADS-1000W ADS-1500W. **CVE ID: CVE-2017-7588**		
Cisco					
Aironet Access Point Cisco Aironet 3500 Series Access Points with CleanAir technology create a self-healing, self-optimizing 802.11n wireless network.					
Gain Privileges	07-04-2017	7.2	A vulnerability in login authentication management in Cisco Aironet 1800, 2800, and 3800 Series Access Point platforms could allow an authenticated, local attacker to gain unrestricted root access to the underlying Linux operating system. The root Linux shell is provided for advanced troubleshooting and should not be available to individual users, even those with root privileges. The attacker must have the root password to exploit this vulnerability. More Information: CSCvb13893. Known Affected Releases: 8.2(121.0) 8.3(102.0). Known Fixed Releases: 8.4(1.53) 8.4(1.52) 8.3(111.0) 8.3(104.23) 8.2(130.0) 8.2(124.1). **CVE ID: CVE-2016-9196**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-aironet	O-CIS-AIRON-200417/396

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

Aironet Access Point Firmware Cisco Aironet 3500 Series Access Points with CleanAir technology create a self-healing, self-optimizing 802.11n wireless network.					
NA	06-04-2017	10	A vulnerability in Cisco Aironet 1830 Series and Cisco Aironet 1850 Series Access Points running Cisco Mobility Express Software could allow an unauthenticated, remote attacker to take complete control of an affected device. The vulnerability is due to the existence of default credentials for an affected device that is running Cisco Mobility Express Software, regardless of whether the device is configured as a master, subordinate, or standalone access point. An attacker who has layer 3 connectivity to an affected device could use Secure Shell (SSH) to log in to the device with elevated privileges. A successful exploit could allow the attacker to take complete control of the device. This vulnerability affects Cisco Aironet 1830 Series and Cisco Aironet 1850 Series Access Points that are running an 8.2.x release of Cisco Mobility Express Software prior to Release 8.2.111.0, regardless of whether the device is configured as a master, subordinate, or standalone access point. Release 8.2 was the first release of Cisco Mobility Express Software for next generation Cisco Aironet Access Points. Cisco Bug IDs: CSCva50691.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ame	O-CIS-AIRON-200417/397

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 ID: CVE-2017-3834**		
Asr 900 Series Firmware NA					
DoS	07-04-2017	6.1	A vulnerability in Cisco ASR 903 or ASR 920 Series Devices running with an RSP2 card could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on a targeted system because of incorrect IPv6 Packet Processing. More Information: CSCuy94366. Known Affected Releases: 15.4(3)S3.15. Known Fixed Releases: 15.6(2)SP 15.6(1.31)SP. **CVE ID: CVE-2017-6603**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-asr	O-CIS-ASR9-200417/398
Ios Xe IOS XE is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), introduced with the ASR 1000 series.					
Execute Code	07-04-2017	6.9	A vulnerability in a startup script of Cisco IOS XE Software could allow an unauthenticated attacker with physical access to the targeted system to execute arbitrary commands on the underlying operating system with the privileges of the root user. More Information: CSCuz06639 CSCuz42122. Known Affected Releases: 15.6(1.1)S 16.1.2 16.2.0 15.2(1)E. Known Fixed Releases: Denali-16.1.3 16.2(1.8) 16.1(2.61) 15.6(2)SP 15.6(2)S1 15.6(1)S2 15.5(3)S3a 15.5(3)S3 15.5(2)S4 15.5(1)S4 15.4(3)S6a 15.4(3)S6 15.3(3)S8a 15.3(3)S8 15.2(5)E 15.2(4)E3 15.2(3)E5	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-iosxe	O-CIS-IOS X-200417/399

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**										

			15.0(2)SQD3 15.0(1.9.2)SQD3 3.9(0)E. **CVE ID: CVE-2017-6606**		
Ios Xr IOS XR is a train of Cisco Systems' widely deployed Internetworking Operating System (IOS), used on their high-end Network Converging System(NCS), carrier-grade routers such as the CRS series, 12000 series, and ASR9000 series.					
DoS; Gain Information	07-04-2017	5	A vulnerability in Google-defined remote procedure call (gRPC) handling in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Event Management Service daemon (emsd) to crash due to a system memory leak, resulting in a denial of service (DoS) condition. This vulnerability affects Cisco IOS XR Software with gRPC enabled. More Information: CSCvb14433. Known Affected Releases: 6.1.1.BASE 6.2.1.BASE. Known Fixed Releases: 6.2.1.22i.MGBL 6.1.22.9i.MGBL 6.1.21.12i.MGBL 6.1.2.13i.MGBL. **CVE ID: CVE-2017-6599**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-ios	O-CIS-IOS X-200417/400
Wireless Lan Controller Firmware NA					
DoS	06-04-2017	7.8	A vulnerability in the web management interface of Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a missing internal handler for the specific request. An attacker could exploit this vulnerability by accessing a specific hidden URL on the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc3	O-CIS-WIREL-200417/401

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

			GUI web management interface. A successful exploit could allow the attacker to cause a reload of the device, resulting in a DoS condition. This vulnerability affects only the Cisco Wireless LAN Controller 8.3.102.0 release. Cisco Bug IDs: CSCvb48198. **CVE ID: CVE-2017-3832**		
NA	06-04-2017	7.8	A vulnerability with IPv6 UDP ingress packet processing in Cisco Wireless LAN Controller (WLC) Software could allow an unauthenticated, remote attacker to cause an unexpected reload of the device. The vulnerability is due to incomplete IPv6 UDP header validation. An attacker could exploit this vulnerability by sending a crafted IPv6 UDP packet to a specific port on the targeted device. An exploit could allow the attacker to impact the availability of the device as it could unexpectedly reload. This vulnerability affects Cisco Wireless LAN Controller (WLC) running software version 8.2.121.0 or 8.3.102.0. Cisco Bug IDs: CSCva98592. **CVE ID: CVE-2016-9219**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170405-wlc2	O-CIS-WIREL-200417/402
Dataprobe					
Ibootbar Firmware iBootBar, a web-accessible, managed PDU for eight independently controlled outlets, enables multiple users to reboot remotely from anywhere, using any web browser, Telnet client or SNMP manager.					
Bypass	07-04-2017	7.5	Dataprobe iBootBar (with 2007-09-20 and possibly later beta firmware) allows remote attackers to bypass authentication, and conduct	http://blog.tmcnet.com/blog/tom-keating/computer-	O-DAT-IBOOT-200417/403

			power-cycle attacks on connected devices, via a DCCOOKIE cookie. **CVE ID: CVE-2007-6760**	hardware/dataprobe-ibootbar-review.asp	
Bypass	07-04-2017	7.5	Dataprobe iBootBar (with 2007-09-20 and possibly later released firmware) allows remote attackers to bypass authentication, and conduct power-cycle attacks on connected devices, via a DCRABBIT cookie. **CVE ID: CVE-2007-6759**	http://blog.tmcnet.com/blog/tom-keating/computer-hardware/dataprobe-ibootbar-review.asp	O-DAT-IBOOT-200417/404
Dell					
Integrated Remote Access Controller Firmware An integrated Dell Remote Access Controller (iDRAC) with Lifecycle Controller is embedded in every Dell PowerEdge server. It provides functionality that helps you deploy, update, monitor and maintain Dell PowerEdge servers with or without a systems management software agent.					
XSS	09-04-2017	4.3	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.85 and 7/8 before 2.30.30.30 has XSS. **CVE ID: CVE-2015-7275**	NA	O-DEL-INTEG-200417/405
Directory Traversal	09-04-2017	4.6	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 and 7/8 before 2.21.21.21 allows directory traversal. **CVE ID: CVE-2015-7270**	NA	O-DEL-INTEG-200417/406
Execute Code	09-04-2017	6.5	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 allows remote attackers to execute arbitrary administrative HTTP commands. **CVE ID: CVE-2015-7274**	NA	O-DEL-INTEG-200417/407
NA	09-04-2017	7.5	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has XXE. **CVE ID: CVE-2015-7273**	http://en.community.dell.com/techcenter/extras/m/white_papers/20441859	O-DEL-INTEG-200417/408
DoS; Overflow	09-04-2017	7.5	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 and 7/8 before 2.21.21.21 allows attackers	NA	O-DEL-INTEG-200417/409

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 cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long SSH username or input. **CVE ID: CVE-2015-7272**		
NA	09-04-2017	7.5	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has a format string issue in racadm getsystinfo. **CVE ID: CVE-2015-7271**	NA	O-DEL-INTEG-200417/410
Dlink					
Dwr-116 Firmware NA					
Directory Traversal	10-04-2017	5	Directory traversal vulnerability in the web interface on the D-Link DWR-116 device with firmware before V1.05b09 allows remote attackers to read arbitrary files via a .. (dot dot) in a "GET /uir/" request. **CVE ID: CVE-2017-6190**	NA	O-DLI-DWR-1-200417/411
CSRF	04-04-2017	6.8	D-Link DIR-615 HW: T1 FW:20.09 is vulnerable to Cross-Site Request Forgery (CSRF) vulnerability. This enables an attacker to perform an unwanted action on a wireless router for which the user/admin is currently authenticated, as demonstrated by changing the Security option from WPA2 to None, or changing the hiddenSSID parameter, SSID parameter, or a security-option password. **CVE ID: CVE-2017-7398**	http://seclists.org/fulldisclosure/2017/Apr/4	O-D-L-DIR-6-200417/412
Dragonwave					
Horizon Wireless Radio Firmware NA					
NA	06-04-2017	7.5	DragonWave Horizon 1.01.03 wireless radios have	http://blog.iancaling.com/	O-DRA-HORIZ-

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

			hardcoded login credentials (such as the username of energetic and password of wireless) meant to allow the vendor to access the devices. These credentials can be used in the web interface or by connecting to the device via TELNET. This is fixed in recent versions including 1.4.8. **CVE ID: CVE-2017-7576**	post/159276197313/	200417/413
Google					
Android Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets.					
Gain Information	06-04-2017	4.3	The high level operating systems (HLOS) was not providing sufficient memory address information to ensure that secure applications inside Qualcomm Secure Execution Environment (QSEE) only write to legitimate memory ranges related to the QSEE secure application's HLOS client. When secure applications inside Qualcomm Secure Execution Environment (QSEE) receive memory addresses from a high level operating system (HLOS) such as Linux Android, those address have previously been verified as belonging to HLOS memory space rather than QSEE memory space, but they were not verified to be from HLOS user space rather than kernel space. This lack of verification could lead to privilege escalation within the HLOS.	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/414

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 ID: CVE-2016-5349		
Bypass Gain Information	07-04-2017	4.3	An information disclosure vulnerability in the factory reset process could enable a local malicious attacker to access data from the previous owner. This issue is rated as Moderate due to the possibility of bypassing device protection. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-30681079. **CVE ID: CVE-2017-0560**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/415
Gain Information	07-04-2017	4.3	An information disclosure vulnerability in libskia could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33897722. **CVE ID: CVE-2017-0559**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/416
Gain Information	07-04-2017	4.3	An information disclosure vulnerability in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34056274. **CVE ID: CVE-2017-0558**	https://android.googlesource.com/platform/frameworks/av/+/50358a80b1724f6cf1bcdf003e1abf9cc141b122	O-GOO-ANDRO-200417/417
Gain Information	07-04-2017	4.3	An information disclosure vulnerability in libmpeg2 in	https://android.googleso	O-GOO-ANDRO-

			Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34093073. **CVE ID: CVE-2017-0557**	urce.com/platform/external/libmpeg2/+/227c1f829127405e21dab1664393050c652ef71e	200417/418
Gain Information	07-04-2017	4.3	An information disclosure vulnerability in libmpeg2 in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34093952. **CVE ID: CVE-2017-0556**	https://android.googlesource.com/platform/external/libmpeg2/+/f301cff2c1ddd880d9a2c77b22602a137519867b	O-GOO-ANDRO-200417/419
Gain Information	07-04-2017	4.3	An information disclosure vulnerability in libavc in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33551775. **CVE ID: CVE-2017-0555**	https://android.googlesource.com/platform/external/libavc/+/0b23c81c3dd9ec38f7e6806a3955fed1925541a0	O-GOO-ANDRO-200417/420
Bypass Gain Information	07-04-2017	4.3	An information disclosure vulnerability in libmedia in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it is	https://android.googlesource.com/platform/frameworks/av/+/9667e3eff2d34c3797c3b	O-GOO-ANDRO-200417/421

			a general bypass for operating system protections that isolate application data from other applications. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33861560. **CVE ID: CVE-2017-0547**	529370de47b2c1f1bf6	
Gain Privileges	07-04-2017	6.8	An elevation of privilege vulnerability in the Telephony component could enable a local malicious application to access capabilities outside of its permission levels. This issue is rated as Moderate because it could be used to gain access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33815946. **CVE ID: CVE-2017-0554**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/422
DoS	07-04-2017	7.1	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097915. **CVE ID: CVE-2017-0552**	https://android.googlesource.com/platform/external/libavc/+/9a00f562a612d56e7b2b989d168647db900ba6cf	O-GOO-ANDRO-200417/423
DoS	07-04-2017	7.1	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/424

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

			rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097231. **CVE ID: CVE-2017-0551**		
DoS	07-04-2017	7.1	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33933140. **CVE ID: CVE-2017-0550**	https://android.googlesource.com/platform/external/libavc/+/7950bf47b6944546a0aff11a7184947de9591b51	O-GOO-ANDRO-200417/425
DoS	07-04-2017	7.1	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33818508. **CVE ID: CVE-2017-0549**	https://android.googlesource.com/platform/external/libavc/+/37345554fea84afd446d6d8fbb87feea5a0dde3f	O-GOO-ANDRO-200417/426
DoS	07-04-2017	7.1	A remote denial of service vulnerability in libskia could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33251605. **CVE ID: CVE-2017-0548**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/427
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the DTS	https://source.android.co	O-GOO-ANDRO-

			sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-33964406. **CVE ID: CVE-2017-0578**	m/security/bulletin/01-04-2017	200417/428
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the MediaTek camera driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28470975. References: M-ALPS02696367. **CVE ID: CVE-2017-0566**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/429
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28175904. References: M-ALPS02696516. **CVE ID: CVE-2017-0565**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/430
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute	https://source.android.com/security/bulletin/01-	O-GOO-ANDRO-200417/431

			arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065. **CVE ID: CVE-2017-0553**	04-2017	
Execute Code	07-04-2017	9.3	An elevation of privilege vulnerability in the MediaTek touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-30202425. References: M-ALPS02898189. **CVE ID: CVE-2017-0562**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/432
Execute Code Gain Privileges	07-04-2017	9.3	An elevation of privilege vulnerability in SurfaceFlinger could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions:	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/433

			4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32628763. **CVE ID: CVE-2017-0546**		
Execute Code Gain Privileges	07-04-2017	9.3	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32591350. **CVE ID: CVE-2017-0545**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/434
Execute Code	07-04-2017	9.3	An elevation of privilege vulnerability in CameraBase could enable a local malicious application to execute arbitrary code. This issue is rated as High because it is a local arbitrary code execution in a privileged process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31992879. **CVE ID: CVE-2017-0544**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/435
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/436

			process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097866. **CVE ID: CVE-2017-0543**		
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33934721. **CVE ID: CVE-2017-0542**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/437
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in sonivox in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34031018. **CVE ID: CVE-2017-0541**	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/438
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the	https://source.android.com/security/bulletin/01-04-2017	O-GOO-ANDRO-200417/439

			context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33966031. **CVE ID: CVE-2017-0540**		
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33864300. **CVE ID: CVE-2017-0539**	https://android.googlesource.com/platform/external/libhevc/+/1ab5ce7e42feccd49e49752e6f58f9097ac5d254	O-GOO-ANDRO-200417/440
Execute Code Overflow Memory Corruption	07-04-2017	9.3	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33641588. **CVE ID: CVE-2017-0538**	https://android.googlesource.com/platform/external/libavc/+/494561291a503840f385fbcd11d9bc5f4dc502b8	O-GOO-ANDRO-200417/441
Google;Linux					
Android/Linux Kernel Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touchscreen mobile devices such as smartphones and tablets/ The Linux kernel is a monolithic Unix-like computer operating system kernel.					
Gain Privileges	04-04-2017	9.3	The eCryptfs subsystem in the Linux kernel before 3.18 allows local users to gain	http://git.kernel.org/cgit/linux/kernel/	O-GOO-ANDRO-200417/442

			privileges via a large filesystem stack that includes an overlayfs layer, related to fs/ecryptfs/main.c and fs/overlayfs/super.c. **CVE ID: CVE-2014-9922**	git/torvalds/linux.git/commit/?id=69c433ed2ecd2d3264efd7afec4439524b319121	
Execute Code	04-04-2017	10	udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag. **CVE ID: CVE-2016-10229**	https://github.com/torvalds/linux/commit/197c949e7798fbf28cfadc69d9ca0c2abbf93191	O-GOO-ANDRO-200417/443
Huawei					
Gain Information	02-04-2017	5	Huawei S9300, S9303, S9306, S9312 with software V100R002; S7700, S7703, S7706, S7712 with software V100R003, V100R006, V200R001, V200R002, V200R003, V200R005; S9300E, S9303E, S9306E, S9312E with software V200R001; S9700, S9703, S9706, S9712 with software V200R002, V200R003, V200R005; S12708, S12712 with software V200R005; 5700HI, 5300HI with software V100R006, V200R001, V200R002, V200R003, V200R005; 5710EI, 5310EI with software V200R002, V200R003, V200R005; 5710HI, 5310HI with software V200R003, V200R005; 6700EI, 6300EI with software V200R005 could cause a leak of IP addresses of devices, related to unintended interface	http://www.huawei.com/en/psirt/security-advisories/hw-372145	O-HUA-5300H-200417/444

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

			support for VRP MPLS LSP Ping. **CVE ID: CVE-2014-8570**		
DoS	02-04-2017	7.8	Huawei AC6605 with software V200R001C00; AC6605 with software V200R002C00; ACU with software V200R001C00; ACU with software V200R002C00; S2300, S3300, S2700, S3700 with software V100R006C05 and earlier versions; S5300, S5700, S6300, S6700 with software V100R006, V200R001, V200R002, V200R003, V200R005C00SPC300 and earlier versions; S7700, S9300, S9300E, S9700 with software V100R006, V200R001, V200R002, V200R003, V200R005C00SPC300 and earlier versions could allow remote attackers to send a special SSH packet to the VRP device to cause a denial of service. **CVE ID: CVE-2014-8572**	http://www.huawei.com/en/psirt/security-advisories/hw-373182	O-HUA-AC660-200417/445
NA	02-04-2017	6	Huawei switches S5700, S6700, S7700, S9700 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300, V200R005C00SPC500, V200R006C00; S12700 with software V200R005C00SPC500, V200R006C00; ACU2 with software V200R005C00SPC500, V200R006C00 have a permission control vulnerability. If a switch enables Authentication,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160217-01-switch-en	O-HUA-ACU2-200417/446

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

			Authorization, and Accounting (AAA) for permission control and user permissions are not appropriate, AAA users may obtain the virtual type terminal (VTY) access permission, resulting in privilege escalation. **CVE ID: CVE-2016-2404**		
NA	02-04-2017	5	Huawei AR3200 with software V200R007C00, V200R005C32, V200R005C20; S12700 with software V200R008C00, V200R007C00; S5300 with software V200R008C00, V200R007C00, V200R006C00; S5700 with software V200R008C00, V200R007C00, V200R006C00; S6300 with software V200R008C00, V200R007C00; S6700 with software V200R008C00, V200R007C00; S7700 with software V200R008C00, V200R007C00, V200R006C00; S9300 with software V200R008C00, V200R007C00, V200R006C00; and S9700 with software V200R008C00, V200R007C00, V200R006C00 allow remote attackers to send abnormal Multiprotocol Label Switching (MPLS) packets to cause memory exhaustion. **CVE ID: CVE-2016-8797**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160608-01-mpls-en	O-HUA-AR320-200417/447
Gain Information	02-04-2017	4.3	Apps on Huawei Ascend P6 mobile phones with software EDGE-U00 V100R001C17B508SP01 and earlier versions before V100R001C17B508SP02;	http://www.huawei.com/en/psirt/security-advisories/hw-372118	O-HUA-ASCEN-200417/448

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

			EDGE-T00 V100R001C01B508SP01 and earlier versions before V100R001C01B508SP02; EDGE-C00 V100R001C92B508SP02 and earlier versions before V100R001C92B508SP03 can capture screens without the root permission. As a result, user information can be leaked by malware on Ascend P6 mobile phones. **CVE ID: CVE-2014-8571**		
DoS Overflow	02-04-2017	7.8	Huawei Campus S3700HI with software V200R001C00SPC300; Campus S5700 with software V200R002C00SPC100; Campus S7700 with software V200R003C00SPC300,V200R003C00SPC500; LSW S9700 with software V200R001C00SPC300,V200R003C00SPC300,V200R003C00SPC500; S2350 with software V200R003C00SPC300; S2750 with software V200R003C00SPC300; S5300 with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S5700 with software V200R001C00SPC300,V200R003C00SPC300; S6300 with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S6700 S3300HI with software V200R001C00SPC300,V200R002C00SPC100,V200R003C00SPC300; S7700 with	http://www.huawei.com/en/psirt/security-advisories/hw-343218	O-HUA-CAMPU-200417/449

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

			software V200R001C00SPC300; S9300 with software V200R001C00SPC300,V200R003C00SPC300,V200R003C00SPC500; S9300E with software V200R003C00SPC300,V200R003C00SPC500 allow attackers to keep sending malformed packets to cause a denial of service (DoS) attack, aka a heap overflow. **CVE ID: CVE-2014-4706**		
Bypass	02-04-2017	7.5	Huawei Campus S7700 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300; S9300 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300; S9700 with software V200R001C00SPC300, V200R002C00SPC100, V200R003C00SPC300 allow unauthorized users to upgrade the bootrom or bootload software, bypass a Menu protection mechanism, conduct a Menu compromise attack, or bypass a Menu/upgrade protection mechanism. **CVE ID: CVE-2014-4707**	http://www.huawei.com/en/psirt/security-advisories/hw-334629	O-HUA-CAMPU-200417/450
Overflow	02-04-2017	5.5	Huawei CloudEngine 5800 with software before V200R001C00SPC700, CloudEngine 6800 with software before V200R001C00SPC700, CloudEngine 7800 with software before V200R001C00SPC700, CloudEngine 8800 with software before	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-cfm-en	O-HUA-CLOUD-200417/451

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

			V200R001C00SPC700, CloudEngine 12800 with software before V200R001C00SPC700 could allow the attacker to exploit a buffer overflow vulnerability by sending crafted packets to the affected system to cause a main control board reboot. **CVE ID: CVE-2016-8790**		
Overflow	02-04-2017	7.1	Huawei CloudEngine 12800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 5800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 6800 with software V100R002C00, V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 7800 with software V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00; CloudEngine 8800 with software V100R006C00; and Secospace USG6600 with software V500R001C00 allow remote unauthenticated attackers to craft specific IPFPM packets to trigger an integer	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-01-vrp-en	O-HUA-CLOUD-200417/452

			overflow and cause the device to reset. **CVE ID: CVE-2016-8795**		
NA	02-04-2017	6.8	Huawei CloudEngine 6800 V100R006C00, CloudEngine 7800 V100R006C00, CloudEngine 8800 V100R006C00, and CloudEngine 12800 V100R006C00 allow remote attackers with specific permission to store massive files to exhaust the shared storage space, leading to a DoS condition. **CVE ID: CVE-2016-8780**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161130-01-switch-en	O-HUA-CLOUD-200417/453
DoS	02-04-2017	4.9	Huawei MBB (Mobile Broadband) product E3272s with software versions earlier than E3272s-153TCPU-V200R002B491D09SP00C00 has a Denial of Service (DoS) vulnerability. An attacker could send a malicious packet to the Common Gateway Interface (CGI) of a target device and make it fail while setting the port attribute, which causes a DoS attack. **CVE ID: CVE-2015-7847**	http://www.huawei.com/en/psirt/security-advisories/hw-450877	O-HUA-E3272-200417/454
Gain Information	02-04-2017	5	Huawei eSpace IAD V300R002C01SPC100 and earlier versions have an information leak vulnerability; an attacker can check and download the fault information by accessing a special URL. **CVE ID: CVE-2016-8271**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160905-01-espace-en	O-HUA-ESPAC-200417/455
XSS Gain Information	02-04-2017	4.3	Huawei eSpace Integrated Access Device (IAD) with software V300R001C03, V300R001C04, V300R001C06, V300R001C20, and	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-ESPAC-200417/456

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

			V300R001C07 allows an attacker to trick a user into clicking a URL containing malicious scripts to obtain user information or hijack the session, aka XSS. **CVE ID: CVE-2016-8789**	20161130-01-espace-en	
NA	02-04-2017	5	Huawei Eudemon8000E firewall with software V200R001C01SPC800 and earlier versions allows users to log in to the device using Telnet or SSH. When an attacker sends to the device a mass of TCP packets with special structure, the logging process becomes slow and users may be unable to log in to the device. **CVE ID: CVE-2014-3221**	http://www.huawei.com/en/psirt/security-advisories/hw-325385	O-HUA-EUDEM-200417/457
NA	02-04-2017	9.3	Huawei Honor 6, Honor 6 Plus, Honor 7 phones with software versions earlier than 6.9.16 could allow attackers to disable the PXN defense mechanism by invoking related drive code to crash the system or escalate privilege. **CVE ID: CVE-2016-8768**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161026-01-pxn-en	O-HUA-HONOR-200417/458
Overflow	02-04-2017	9.3	Video driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and Huawei Honor 6 phones with software versions before H60-L02_6.10.1 has a stack overflow vulnerability, which allows attackers to crash the system or escalate user privilege. **CVE ID: CVE-2016-8761**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161012-01-smartphone-en	O-HUA-HONOR-200417/459
Overflow	02-04-2017	9.3	Touchscreen driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and	http://www.huawei.com/en/psirt/security-	O-HUA-HONOR-200417/460

			Huawei Honor 6 phones with software versions before H60-L02_6.10.1 has a heap overflow vulnerability, which allows attackers to crash the system or escalate user privilege. **CVE ID: CVE-2016-8760**	advisories/huawei-sa-20161012-01-smartphone-en	
Overflow	02-04-2017	9.3	Video driver in Huawei P9 phones with software versions before EVA-AL10C00B192 and Huawei Honor 6 phones with software versions before H60-L02_6.10.1 has a stack overflow vulnerability, which allows attackers to crash the system or escalate user privilege. **CVE ID: CVE-2016-8759**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161012-01-smartphone-en	O-HUA-HONOR-200417/461
DoS	02-04-2017	7.1	ION memory management module in Huawei Mate8 phones with software NXT-AL10C00B561 and earlier versions, NXT-CL10C00B561 and earlier versions, NXT-DL10C00B561 and earlier versions, NXT-TL10C00B561 and earlier versions allows attackers to cause a denial of service (restart). **CVE ID: CVE-2016-8758**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20170111-01-smartphone-en	O-HUA-MATE -200417/462
DoS	02-04-2017	7.1	ION memory management module in Huawei Mate 8 phones with software NXT-AL10C00B197 and earlier versions, NXT-DL10C00B197 and earlier versions, NXT-TL10C00B197 and earlier versions, NXT-CL10C00B197 and earlier versions allows attackers to cause a denial of service (restart).	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161026-01-smartphone-en	O-HUA-MATE -200417/463

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 ID: CVE-2016-8756		
NA	02-04-2017	6.2	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege. **CVE ID: CVE-2016-8794**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-smartphone-en	O-HUA-MATE -200417/464
NA	02-04-2017	6.2	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-smartphone-en	O-HUA-MATE -200417/465

			Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege. **CVE ID: CVE-2016-8793**		
NA	02-04-2017	6.2	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege. **CVE ID: CVE-2016-8792**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-smartphone-en	O-HUA-MATE -200417/466

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	02-04-2017	6.2	Huawei Mate 8 phones with software Versions before NXT-AL10C00B386, Versions before NXT-CL00C92B386, Versions before NXT-DL00C17B386, Versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368, Versions before CRR-UL20C00B368; and P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366 allow attackers with graphic or Camera privilege to crash the system or escalate privilege. **CVE ID: CVE-2016-8791**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161116-01-smartphone-en	O-HUA-MATE -200417/467
Execute Code Overflow	02-04-2017	7.2	The HIFI driver in Huawei Mate 8 phones with software versions before NXT-AL10C00B386, versions before NXT-CL00C92B386, versions before NXT-DL00C17B386, versions before NXT-TL00C01B386; Mate S phones with software Versions before CRR-CL00C92B368, Versions before CRR-CL20C92B368, Versions before CRR-TL00C01B368, Versions before CRR-UL00C00B368,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-02-smartphone-en	O-HUA-MATE -200417/468

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

			Versions before CRR-UL20C00B368; P8 phones with software Versions before GRA-TL00C01B366, Versions before GRA-CL00C92B366, Versions before GRA-CL10C92B366, Versions before GRA-UL00C00B366, Versions before GRA-UL10C00B366; and P9 phones with software Versions before EVA-AL10C00B190, Versions before EVA-DL10C00B190, Versions before EVA-TL10C00B190, Versions before EVA-CL10C00B190 allows attackers to get root privilege or crash the system or execute arbitrary code, related to a buffer overflow. **CVE ID: CVE-2016-8774**		
Execute Code Overflow	02-04-2017	7.2	Touch Panel (TP) driver in Huawei NEM phones with software Versions before NEM-AL10C00B130, Versions before NEM-UL10C17B160, Versions before NEM-UL10C00B160, Versions before NEM-TL00C01B160 allows attackers to get root privilege or crash the system or execute arbitrary code, related to a buffer overflow. **CVE ID: CVE-2016-8775**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-03-smartphone-en	O-HUA-NEM-A-200417/469
NA	02-04-2017	5.4	Huawei OceanStor 5600 V3 V300R003C00 has a hardcoded SSH key vulnerability; the hardcoded keys are used to encrypt communication data and authenticate different nodes of the devices. An attacker	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161017-01-storage-	O-HUA-OCEAN-200417/470

			may obtain the hardcoded keys and log in to such a device through SSH. **CVE ID: CVE-2016-8754**	en	
NA	02-04-2017	9	Huawei OceanStor 5600 V3 with V300R003C00C10 and earlier versions allows attackers with administrator privilege to inject a command into a specific command's parameters, and run this injected command with root privilege. **CVE ID: CVE-2016-8801**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161207-01-storage-en	O-HUA-OCEAN-200417/471
Overflow	02-04-2017	4	The Huawei OceanStor 5800 V300R003C00 has an integer overflow vulnerability. An authenticated attacker may send massive abnormal Network File System (NFS) packets, causing an anomaly in specific disk arrays. **CVE ID: CVE-2016-6177**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20160629-02-oceanstor-en	O-HUA-OCEAN-200417/472
Gain Information	02-04-2017	4.3	The MeWidget module on Huawei P7 smartphones with software P7-L10 V100R001C00B136 and earlier versions could lead to the disclosure of contact information. **CVE ID: CVE-2015-2246**	http://www.huawei.com/en/psirt/security-advisories/hw-414289	O-HUA-P7-L1-200417/473
NA	02-04-2017	1.9	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an input validation vulnerability, which allows attackers to cause the system to restart. **CVE ID: CVE-2016-8762**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-01-smartphone-en	O-HUA-P8 LI-200417/474

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	02-04-2017	4.1	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an input validation vulnerability, which allows attackers to read and write user-mode memory data anywhere in the TrustZone driver. **CVE ID: CVE-2016-8764**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-01-smartphone-en	O-HUA-P8 LI-200417/475
NA	02-04-2017	9.3	The TrustZone driver in Huawei P9 phones with software Versions earlier than EVA-AL10C00B352 and P9 Lite with software VNS-L21C185B130 and earlier versions and P8 Lite with software ALE-L02C636B150 and earlier versions has an improper resource release vulnerability, which allows attackers to cause a system restart or privilege elevation. **CVE ID: CVE-2016-8763**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161123-01-smartphone-en	O-HUA-P8 LI-200417/476
Gain Information	02-04-2017	4.3	ION memory management module in Huawei P9 phones with software EVA-AL10C00B192 and earlier versions, EVA-DL10C00B192 and earlier versions, EVA-TL10C00B192 and earlier versions, EVA-CL10C00B192 and earlier versions allows attackers to obtain sensitive information from uninitialized memory. **CVE ID: CVE-2016-8757**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161026-02-smartphone-en	O-HUA-P9 FI-200417/477

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**										

Bypass	02-04-2017	2.1	Huawei P9 phones with software EVA-AL10C00,EVA-CL10C00,EVA-DL10C00,EVA-TL10C00 and P9 Lite phones with software VNS-L21C185 allow attackers to bypass the factory reset protection (FRP) to enter some functional modules without authorization and perform operations to update the Google account. **CVE ID: CVE-2016-8776**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161207-01-smartphone-en	O-HUA-P9 FI-200417/478
NA	02-04-2017	7.8	Huawei Quidway S9700 V200R003C00SPC500, Quidway S9300 V200R003C00SPC500, Quidway S7700 V200R003C00SPC500, Quidway S6700 V200R003C00SPC300, Quidway S6300 V200R003C00SPC300, Quidway S5700 V200R003C00SPC300, Quidway S5300 V200R003C00SPC300 enable attackers to launch DoS attacks by crafting and sending malformed packets to these vulnerable products. **CVE ID: CVE-2014-3224**	http://www.huawei.com/en/psirt/security-advisories/hw-333184	O-HUA-QUIDW-200417/479
DoS	02-04-2017	5	Huawei S5300 with software V200R003C00, V200R007C00, V200R008C00, V200R009C00; S5700 with software V200R001C00, V200R002C00, V200R003C00, V200R005C00, V200R005C03, V200R007C00, V200R008C00,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161111-01-mpls-en	O-HUA-S1270-200417/480

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

			V200R009C00; S6300 with software V200R003C00, V200R005C00, V200R008C00, V200R009C00; S6700 with software V200R001C00, V200R001C01, V200R002C00, V200R003C00, V200R005C00, V200R008C00, V200R009C00; S7700 with software V200R007C00, V200R008C00, V200R009C00; S9300 with software V200R007C00, V200R008C00, V200R009C00; S9700 with software V200R007C00, V200R008C00, V200R009C00; and S12700 with software V200R007C00, V200R007C01, V200R008C00, V200R009C00 allow the attacker to cause a denial of service condition by sending malformed MPLS packets. **CVE ID: CVE-2016-8773**		
NA	02-04-2017	7.8	Huawei S9300 with software before V100R006SPH013 and S2300,S3300,S5300,S6300 with software before V100R006SPH010 support Y.1731 and therefore have the Y.1731 vulnerability in processing special packets. The vulnerability causes the restart of switches. **CVE ID: CVE-2014-3223**	http://www.huawei.com/en/psirt/security-advisories/hw-329625	O-HUA-S2300-200417/481
NA	02-04-2017	4	Huawei Secospace USG6300 with software V500R001C20 and V500R001C20SPC200PWE, Secospace USG6500 with	http://www.huawei.com/en/psirt/security-advisories/h	O-HUA-SECOS-200417/482

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

			software V500R001C20, Secospace USG6600 with software V500R001C20 and V500R001C20SPC200PWE allow remote attackers with specific permission to log in to a device and deliver a large number of unspecified commands to exhaust memory, causing a DoS condition. **CVE ID: CVE-2016-8781**	uawei-sa-20161214-01-firewall-en	
Overflow	02-04-2017	6.8	The security policy processing module in Huawei Secospace USG6300 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200; Secospace USG6500 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200; Secospace USG6600 with software V500R001C20SPC100, V500R001C20SPC101, V500R001C20SPC200 allows authenticated attackers to setup a specific security policy into the devices, causing a buffer overflow and crashing the system. **CVE ID: CVE-2016-8802**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161125-01-usg-en	O-HUA-SECOS-200417/483
Gain Information	02-04-2017	4	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal	http://www.huawei.com/en/psirt/security-advisories/hw-408100	O-HUA-TECAL-200417/484

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

		🟩	RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2		

			V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions could allow users who log in to the products to view the sessions IDs of all online users on the Online Users page of the web UI. **CVE ID: CVE-2014-9691**		
Gain Information	02-04-2017	5	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and	http://www.huawei.com/en/psirt/security-advisories/hw-408100	O-HUA-TECAL-200417/485

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

		🟨	earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and		

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

			earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions could allow attackers to figure out the RMCP+ session IDs of users and access the system with forged identities. **CVE ID: CVE-2014-9692**		
CSRF	02-04-2017	6.8	Huawei Tecal RH1288 V2 V100R002C00SPC107 and	http://www. huawei.com/	O-HUA-TECAL-

			earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2	en/psirt/security-advisories/hw-408100	200417/486

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

		🟧	V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240 V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions have a CSRF vulnerability. The products do not use the Token mechanism for web access		

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

			control. When users log in to the Huawei servers and access websites containing the malicious CSRF script, the CSRF script is executed, which may cause configuration tampering and system restart. **CVE ID: CVE-2014-9694**		
Execute Code	02-04-2017	7.5	Huawei Tecal RH1288 V2 V100R002C00SPC107 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285 V2 V100R002C00SPC115 and earlier versions, Tecal RH2265 V2 V100R002C00, Tecal RH2285H V2 V100R002C00SPC111 and earlier versions, Tecal RH2268 V2 V100R002C00, Tecal RH2288 V2 V100R002C00SPC117 and earlier versions, Tecal RH2288H V2 V100R002C00SPC115 and earlier versions, Tecal RH2485 V2 V100R002C00SPC502 and earlier versions, Tecal RH5885 V2 V100R001C02SPC109 and earlier versions, Tecal RH5885 V3 V100R003C01SPC102 and earlier versions, Tecal RH5885H V3 V100R003C00SPC102 and earlier versions, Tecal XH310 V2 V100R001C00SPC110 and earlier versions, Tecal XH311 V2 V100R001C00SPC110 and earlier versions, Tecal XH320 V2 V100R001C00SPC110 and	http://www.huawei.com/en/psirt/security-advisories/hw-408100	O-HUA-TECAL-200417/487

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

		🟧	earlier versions, Tecal XH621 V2 V100R001C00SPC106 and earlier versions, Tecal DH310 V2 V100R001C00SPC110 and earlier versions, Tecal DH320 V2 V100R001C00SPC106 and earlier versions, Tecal DH620 V2 V100R001C00SPC106 and earlier versions, Tecal DH621 V2 V100R001C00SPC107 and earlier versions, Tecal DH628 V2 V100R001C00SPC107 and earlier versions, Tecal BH620 V2 V100R002C00SPC107 and earlier versions, Tecal BH621 V2 V100R002C00SPC106 and earlier versions, Tecal BH622 V2 V100R002C00SPC110 and earlier versions, Tecal BH640 V2 V100R002C00SPC108 and earlier versions, Tecal CH121 V100R001C00SPC180 and earlier versions, Tecal CH140 V100R001C00SPC110 and earlier versions, Tecal CH220 V100R001C00SPC180 and earlier versions, Tecal CH221 V100R001C00SPC180 and earlier versions, Tecal CH222 V100R002C00SPC180 and earlier versions, Tecal CH240		

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

			V100R001C00SPC180 and earlier versions, Tecal CH242 V100R001C00SPC180 and earlier versions, Tecal CH242 V3 V100R001C00SPC110 and earlier versions could allow attackers to execute arbitrary code or restart the system via crafted DNS packets. **CVE ID: CVE-2014-9693**		
NA	02-04-2017	6.5	The Hyper Module Management (HMM) software of Huawei Tecal E9000 Chassis V100R001C00SPC160 and earlier versions allows the operator to modify the user configuration of iMana through privilege escalation. **CVE ID: CVE-2014-9696**	http://www.huawei.com/en/psirt/security-advisories/hw-408117	O-HUA-TECAL-200417/488
NA	02-04-2017	6.5	The Hyper Module Management (HMM) software of Huawei Tecal E9000 Chassis V100R001C00SPC160 and earlier versions could allow a non-super-domain user who accesses HMM through SNMPv3 to perform operations on a server as a super-domain user. **CVE ID: CVE-2014-9695**	http://www.huawei.com/en/psirt/security-advisories/hw-408118	O-HUA-TECAL-200417/489
DoS Bypass	02-04-2017	7.8	Huawei USG5500 with software V300R001C00 and V300R001C00 allows attackers to bypass the anti-DDoS module of the USGs to cause a denial of service condition on the backend server. **CVE ID: CVE-2016-8798**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161026-01-usg-en	O-HUA-USG55-200417/490
NA	02-04-2017	7.8	Huawei USG9520 V300R001C01, USG9560 V300R001C01, and	http://www.huawei.com/en/psirt/sec	O-HUA-USG95-200417/491

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

			USG9580 V300R001C01 allow unauthenticated attackers to send abnormal DHCP request packets to the affected products to trigger a DoS condition. **CVE ID: CVE-2016-8796**	urity-advisories/huawei-sa-20161116-01-firewall-en	
NA	02-04-2017	5	Huawei home gateways WS318 with software V100R001C01B022 and earlier versions are affected by the PIN offline brute force cracking vulnerability of the WPS protocol because the random number generator (RNG) used in the supplier's solution is not random enough. As a result, brute force cracking the PIN code is easier. After an attacker cracks the PIN, the attacker can access the Internet via the cracked device. **CVE ID: CVE-2014-9690**	http://www.huawei.com/en/psirt/security-advisories/hw-408091	O-HUA-WS318-200417/492
Ibaby					
M3s Baby Monitor Firmware; M6 Baby Monitor Firmware NA					
NA	09-04-2017	10	iBaby M3S has a password of admin for the backdoor admin account. **CVE ID: CVE-2015-2887**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	O-IBA-M3SB-200417/493
Gain Information	09-04-2017	5	iBaby M6 allows remote attackers to obtain sensitive information, related to the ibabycloud.com service. **CVE ID: CVE-2015-2886**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec	O-IBA-M6BA-200417/494

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**										

				-disclosure-10-new-vulns-for-several-video-baby-monitors	
Intel					
Nuc6i3syh Bios;Nuc6i3syk Bios; Nuc6i7kyk Bios; Stk2mv64cc Bios					
NA	03-04-2017	2.1	The BIOS in Intel NUC systems based on 6th Gen Intel Core processors prior to version SY0059 may allow may allow an attacker with physical access to the system to gain access to personal information. **CVE ID: CVE-2017-5686**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00073&languageid=en-fr	O-INT-NUC6I-200417/495
NA	03-04-2017	2.1	The BIOS in Intel NUC systems based on 6th Gen Intel Core processors prior to version KY0045 may allow may allow an attacker with physical access to the system to gain access to personal information. **CVE ID: CVE-2017-5685**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00073&languageid=en-fr	O-INT-NUC6I-200417/496
NA	03-04-2017	2.1	The BIOS in Intel Compute Stick systems based on 6th Gen Intel Core processors prior to version CC047 may allow an attacker with physical access to the system to gain access to personal information. **CVE ID: CVE-2017-5684**	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00073&languageid=en-fr	O-INT-STK2M-200417/497
Jensenofscandinavia					
Al3g Firmware;Al5000ac Firmware;Al59300 Firmware					
Gain Information	03-04-2017	4	Jensen of Scandinavia AS Air:Link 3G (AL3G) version 2.23m (Rev. 3), Air:Link 5000AC (AL5000AC) version 1.13, and Air:Link 59300 (AL59300) version 1.04 (Rev. 4) devices allow remote attackers to read passwords via a direct	https://www.riskbasedsecurity.com/research/RBS-2016-004.pdf	O-JEN-AL3G -200417/498

			request to the x.asp page. **CVE ID: CVE-2016-10314**		
NA	03-04-2017	5.8	Jensen of Scandinavia AS Air:Link 3G (AL3G) version 2.23m (Rev. 3), Air:Link 5000AC (AL5000AC) version 1.13, and Air:Link 59300 (AL59300) version 1.04 (Rev. 4) devices allow remote attackers to conduct Open Redirect attacks via the return-url parameter to /goform/formLogout. **CVE ID: CVE-2016-10316**	https://www.riskbasedsecurity.com/research/RBS-2016-004.pdf	O-JEN-AL3G - 200417/499
NA	03-04-2017	5.8	Jensen of Scandinavia AS Air:Link 3G (AL3G) version 2.23m (Rev. 3), Air:Link 5000AC (AL5000AC) version 1.13, and Air:Link 59300 (AL59300) version 1.04 (Rev. 4) devices allow remote attackers to conduct Open Redirect attacks via the submit-url parameter to certain /goform/* pages. **CVE ID: CVE-2016-10315**	https://www.riskbasedsecurity.com/research/RBS-2016-004.pdf	O-JEN-AL3G - 200417/500
CSRF	03-04-2017	6.8	Jensen of Scandinavia AS Air:Link 3G (AL3G) version 2.23m (Rev. 3), Air:Link 5000AC (AL5000AC) version 1.13, and Air:Link 59300 (AL59300) version 1.04 (Rev. 4) devices allow remote attackers to conduct CSRF attacks via certain /goform/* pages. **CVE ID: CVE-2016-10313**	https://www.riskbasedsecurity.com/research/RBS-2016-004.pdf	O-JEN-AL3G - 200417/501
Execute Code	03-04-2017	10	Jensen of Scandinavia AS Air:Link 3G (AL3G) version 2.23m (Rev. 3), Air:Link 5000AC (AL5000AC) version 1.13, and Air:Link 59300 (AL59300) version 1.04 (Rev. 4) devices allow remote attackers to execute arbitrary commands via shell metacharacters to	https://www.riskbasedsecurity.com/research/RBS-2016-004.pdf	O-JEN-AL3G - 200417/502

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

			certain /goform/* pages. **CVE ID: CVE-2016-10312**		
Lens Laboratories					
Peek-a-view Firmware NA					
NA	09-04-2017	10	Lens Peek-a-View has a password of 2601hx for the backdoor admin account, a password of user for the backdoor user account, and a password of guest for the backdoor guest account. **CVE ID: CVE-2015-2885**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	O-LEN-PEEK--200417/503
Linux					
Linux Kernel The Linux kernel is a monolithic Unix-like computer operating system kernel.					
Gain Information	10-04-2017	2.1	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation. **CVE ID: CVE-2017-7616**	https://github.com/torvalds/linux/commit/cf01fb9985e8deb25ccf0ea54d916b8871ae0e62	O-LIN-LINUX-200417/504
Gain Information	05-04-2017	2.6	An information disclosure vulnerability in the NVIDIA crypto driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10. Android ID: A-33899858. References: N-CVE ID: CVE-2017-0330. **CVE ID: CVE-2017-0330**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/505

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

Gain Information	05-04-2017	2.6	An information disclosure vulnerability in the NVIDIA crypto driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10. Android ID: A-33898322. References: N-CVE ID: CVE-2017-0328. **CVE ID: CVE-2017-0328**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/506
Gain Information	07-04-2017	2.6	An information disclosure vulnerability in the Qualcomm sound driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33649808. References: QC-CR#1097569. **CVE ID: CVE-2017-0586**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/507
Gain Information	07-04-2017	2.6	An information disclosure vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32475556. References: B-RB#112953. **CVE ID: CVE-2017-0585**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/508

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

Gain Information	07-04-2017	2.6	An information disclosure vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32074353. References: QC-CR#1104731. **CVE ID: CVE-2017-0584**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/509
DoS	04-04-2017	4	A missing authorization check in the fscrypt_process_policy function in fs/crypto/policy.c in the ext4 and f2fs filesystem encryption support in the Linux kernel before 4.7.4 allows a user to assign an encryption policy to a directory owned by a different user, potentially creating a denial of service. **CVE ID: CVE-2016-10318**	https://github.com/torvalds/linux/commit/163ae1c6ad6299b19e22b4a35d5ab24a89791a98	O-LIN-LINUX-200417/510
DoS	04-04-2017	4.6	The msm_ipc_router_close function in net/ipc_router/ipc_router_socket.c in the ipc_router component for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact by triggering failure of an accept system call for an AF_MSM_IPC	https://source.codeaurora.org/quic/la//kernel/msm-3.18/commit/?id=71fe5361cbef34e2d606b79e8936a910a3e95566	O-LIN-LINUX-200417/511

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

			socket. **CVE ID: CVE-2016-5870**		
DoS	05-04-2017	4.9	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call. **CVE ID: CVE-2017-2671**	https://git.kernel.org/pub/scm/linux/kernel/git/davem/net.git/commit/net/ipv4/ping.c?id=43a6684519ab0a6c52024b5e25322476cabad893	O-LIN-LINUX-200417/512
Execute Code	05-04-2017	7.6	An elevation of privilege vulnerability in the NVIDIA crypto driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10. Android ID: A-27930566. References: N-CVE-2017-0339. **CVE ID: CVE-2017-0339**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/513
Execute Code	05-04-2017	7.6	An elevation of privilege vulnerability in the NVIDIA crypto driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10. Android ID: A-33812508. References: N-CVE-2017-0332. **CVE ID: CVE-2017-0332**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/514

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

Execute Code	05-04-2017	7.6	An elevation of privilege vulnerability in the NVIDIA boot and power management processor driver could enable a local malicious application to execute arbitrary code within the context of the boot and power management processor. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.18. Android ID:A-34115304. References: N-CVE ID: CVE-2017-0329. **CVE ID: CVE-2017-0329**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/515
Execute Code	05-04-2017	7.6	An elevation of privilege vulnerability in the NVIDIA crypto driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10. Android ID: A-33893669. References: N-CVE ID: CVE-2017-0327. **CVE ID: CVE-2017-0327**	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/516
Execute Code	05-04-2017	7.6	An elevation of privilege vulnerability in the NVIDIA I2C HID driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel 3.10 and Kernel 3.18. Android ID: A-33040280.	https://source.android.com/security/bulletin/01-04-2017.html	O-LIN-LINUX-200417/517

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

			References: N-CVE ID: CVE-2017-0325. **CVE ID: CVE-2017-0325**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm CP access driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and because of vulnerability specific details which limit the impact of the issue. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32068683. References: QC-CR#1103788. **CVE ID: CVE-2017-0583**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/518
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the HTC OEM fastboot command could enable a local malicious application to execute arbitrary code within the context of the sensor hub. This issue is rated as Moderate because it first requires exploitation of separate vulnerabilities. Product: Android. Versions: Kernel-3.10. Android ID: A-33178836. **CVE ID: CVE-2017-0582**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/519
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/520

			requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34614485. **CVE ID: CVE-2017-0581**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34325986. **CVE ID: CVE-2017-0580**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/521
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34125463. References: QC-CR#1115406. **CVE ID: CVE-2017-0579**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/522
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/523

			compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33842951. **CVE ID: CVE-2017-0577**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33544431. References: QC-CR#1103089. **CVE ID: CVE-2017-0576**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/524
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32658595. References: QC-CR#1103099. **CVE ID: CVE-2017-0575**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/525
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/526

			High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34624457. References: B-RB#113189. **CVE ID: CVE-2017-0574**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34469904. References: B-RB#91539. **CVE ID: CVE-2017-0573**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/527
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-34198931. References: B-RB#112597. **CVE ID: CVE-2017-0572**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/528
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/529

			kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34203305. References: B-RB#111541. **CVE ID: CVE-2017-0571**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199963. References: B-RB#110688. **CVE ID: CVE-2017-0570**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/530
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34198729. References: B-RB#110666. **CVE ID: CVE-2017-0569**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/531
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/532

			within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34197514. References: B-RB#112600. **CVE ID: CVE-2017-0568**		
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32125310. References: B-RB#112575. **CVE ID: CVE-2017-0567**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/533
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm Seemp driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33353601. References: QC-CR#1102288. **CVE ID: CVE-2017-0462**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/534
Execute Code	07-04-2017	7.6	An elevation of privilege vulnerability in the Qualcomm audio driver could enable a local malicious application to	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/535

			execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33353700. References: QC-CR#1104067. **CVE ID: CVE-2017-0454**		
DoS	10-04-2017	7.8	crypto/ahash.c in the Linux kernel through 4.10.9 allows attackers to cause a denial of service (API operation calling its own callback, and infinite recursion) by triggering EBUSY on a full queue. **CVE ID: CVE-2017-7618**	NA	O-LIN-LINUX-200417/536
Execute Code	07-04-2017	9.3	An elevation of privilege vulnerability in the kernel ION subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34276203. **CVE ID: CVE-2017-0564**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/537
Execute Code	07-04-2017	9.3	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/538

			to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32089409. **CVE ID: CVE-2017-0563**		
Execute Code	07-04-2017	10	A remote code execution vulnerability in the Broadcom Wi-Fi firmware could enable a remote attacker to execute arbitrary code within the context of the Wi-Fi SoC. This issue is rated as Critical due to the possibility of remote code execution in the context of the Wi-Fi SoC. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199105. References: B-RB#110814. **CVE ID: CVE-2017-0561**	https://source.android.com/security/bulletin/01-04-2017	O-LIN-LINUX-200417/539
Microsoft					
Windows 10;Windows 8.1;Windows Rt 8.1;Windows Server 2012; ;Windows Server 2008; Windows Server 2016; Windows 7; Windows Vista Microsoft Windows (or simply Windows) is a metafamily of graphical operating systems developed, marketed, and sold by Microsoft.					
NA	12-04-2017	7.2	An elevation of privilege vulnerability exists when Microsoft Windows running on Windows 10, Windows 10 1511, Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2 fails to properly sanitize handles in memory, aka "Windows Elevation of Privilege Vulnerability." **CVE ID: CVE-2017-0165**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0165	O-MIC-WINDO-200417/540
Execute Code	12-04-2017	7.4	A remote code execution vulnerability exists when Windows Hyper-V Network	https://portal.msrc.microsoft.com/en-	O-MIC-WINDO-200417/541

			Switch running on a host server fails to properly validate input from an authenticated user on a guest operating system, aka "Hyper-V Remote Code Execution Vulnerability." This CVE ID is unique from CVE ID: CVE-2017-0162, CVE ID: CVE-2017-0180, and CVE ID: CVE-2017-0181. **CVE ID: CVE-2017-0163**	US/security-guidance/advisory/CVE-2017-0163	
Execute Code	12-04-2017	7.4	A remote code execution vulnerability exists when Windows Hyper-V Network Switch running on a Windows 10, Windows 8.1, Windows Server 2012 R2, or Windows Server 2016 host server fails to properly validate input from an authenticated user on a guest operating system, aka "Hyper-V Remote Code Execution Vulnerability." This CVE ID is unique from CVE ID: CVE-2017-0163, CVE ID: CVE-2017-0180, and CVE ID: CVE-2017-0181. **CVE ID: CVE-2017-0162**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0162	O-MIC-WINDO-200417/542
DoS	12-04-2017	3.5	A denial of service vulnerability exists in Windows 10 1607 and Windows Server 2016 Active Directory when an authenticated attacker sends malicious search queries, aka "Active Directory Denial of Service Vulnerability." **CVE ID: CVE-2017-0164**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0164	O-MIC-WINDO-200417/543
Gain Privileges	12-04-2017	6.9	The Graphics component in the kernel in Microsoft Windows Vista SP2; Windows Server 2008 SP2	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WINDO-200417/544

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 R2 SP1; and Windows 7 SP1 allows local users to gain privileges via a crafted application, aka "Windows Graphics Elevation of Privilege Vulnerability." **CVE ID: CVE-2017-0155**	guidance/advisory/CVE-2017-0155	
Nixos Project					
Nixos NixOS is a GNU/Linux distribution that aims to improve the state of the art in system configuration management.					
Gain Privileges	03-04-2017	7.2	NixOS 17.03 before 17.03.887 has a world-writable Docker socket, which allows local users to gain privileges by executing docker commands. **CVE ID: CVE-2017-7412**	https://github.com/NixOS/nixpkgs/commit/fa4fe7110566d8370983fa81f2b04a833339236d	O-NIX-NIXOS-200417/545
Riverbed					
Rios The Riverbed Optimization System (RiOS) is the software platform that powers our award-winning line of SteelHead appliances from Riverbed.					
NA	04-04-2017	1.9	** DISPUTED ** Riverbed RiOS through 9.6.0 has a weak default password for the secure vault, which makes it easier for physically proximate attackers to defeat the secure-vault protection mechanism by leveraging knowledge of the password algorithm and the appliance serial number. NOTE: the vendor believes that this does not meet the definition of a vulnerability. The product contains correct computational logic for supporting arbitrary password changes by customers; however, a password change is optional to meet different customers' needs.	NA	O-RIV-RIOS-200417/546

			CVE ID: CVE-2017-7306		
NA	04-04-2017	2.1	** DISPUTED ** Riverbed RiOS through 9.6.0 does not require a bootloader password, which makes it easier for physically proximate attackers to defeat the secure-vault protection mechanism via a crafted boot. NOTE: the vendor believes that this does not meet the definition of a vulnerability. The product contains correct computational logic for a bootloader password; however, this password is optional to meet different customers' needs. **CVE ID: CVE-2017-7305**	NA	O-RIV-RIOS-200417/547
Gain Information	04-04-2017	2.1	Riverbed RiOS through 9.6.0 deletes the secure vault with the rm program (not shred or srm), which makes it easier for physically proximate attackers to obtain sensitive information by reading raw disk blocks. **CVE ID: CVE-2017-5670**	NA	O-RIV-RIOS-200417/548
NA	04-04-2017	7.2	Riverbed RiOS before 9.0.1 does not properly restrict shell access in single-user mode, which makes it easier for physically proximate attackers to obtain root privileges and access decrypted data by replacing the /opt/tms/bin/cli file. **CVE ID: CVE-2017-7307**	NA	O-RIV-RIOS-200417/549
Schneider-electric					
Conext Combox 865-1058 Firmware The Conext ComBox is a powerful communications and monitoring device for installers and operators of Conext solar systems.					
NA	07-04-2017	7.8	An issue was discovered in	http://downl	O-SCH-

			Schneider Electric Conext ComBox, model 865-1058, all firmware versions prior to V3.03 BN 830. A series of rapid requests to the device may cause it to reboot. **CVE ID: CVE-2017-6019**	oad.schneider-electric.com/files?p_Doc_Ref=SEVD-2017-052-01	CONEX-200417/550
Modicon Tm221ce16r Firmware NA					
Gain Information	06-04-2017	5	Schneider Electric Modicon TM221CE16R 1.3.3.3 devices allow remote attackers to discover the application-protection password via a \x00\x01\x00\x00\x00\x05\x01\x5a\x00\x03\x00 request to the Modbus port (502/tcp). Subsequently the application may be arbitrarily downloaded, modified, and uploaded. **CVE ID: CVE-2017-7575**	http://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2017-097-02	O-SCH-MODIC-200417/551
Sierrawireless					
Aleos Firmware NA					
NA	09-04-2017	5	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 store passwords in cleartext. **CVE ID: CVE-2016-5070**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/552
NA	09-04-2017	7.5	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 use guessable session tokens, which are in the URL. **CVE ID: CVE-2016-5069**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/553
NA	09-04-2017	7.5	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 do not require authentication for Embedded_Ace_Get_Task.cgi requests.	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/554

			CVE ID: CVE-2016-5068		
NA	09-04-2017	7.5	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Embedded_Ace_Set_Task.cgi command injection. **CVE ID: CVE-2016-5065**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/555
NA	09-04-2017	9	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Hayes AT command injection. **CVE ID: CVE-2016-5067**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/556
NA	09-04-2017	10	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 execute the management web application as root. **CVE ID: CVE-2016-5071**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/557
NA	09-04-2017	10	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 have weak passwords for admin, rauser, sconsole, and user. **CVE ID: CVE-2016-5066**	https://carvesystems.com/sierra-wireless-2016-advisory.html	O-SIE-ALEOS-200417/558
Sophos					
Cyberoam Cr25ing Utm Firmware NA					
Bypass	07-04-2017	9	Sophos Cyberoam UTM CR25iNG 10.6.3 MR-5 allows remote authenticated users to bypass intended access restrictions via direct object reference, as demonstrated by a request for Licenseinformation.jsp. This is fixed in 10.6.5. **CVE ID: CVE-2016-7786**	https://infosecninja.blogspot.in/2017/04/CVE ID: CVE-2016-7786-sophos-cyberoam-utm.html	O-SOP-CYBER-200417/559
Summer Infant					
Baby Zoom Wifi Monitor Firmware NA					
Gain Privileges	09-04-2017	6.5	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to gain	https://community.rapid7.com/community/infosec/blo	O-SUM-BABY-200417/560

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**										

			privileges via manual entry of a Settings URL. **CVE ID: CVE-2015-2889**	g/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	
Bypass	09-04-2017	7.5	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to bypass authentication, related to the MySnapCam web service. **CVE ID: CVE-2015-2888**	https://community.rapid7.com/community/infosec/blog/2015/09/02/iotsec-disclosure-10-new-vulns-for-several-video-baby-monitors	O-SUM-BABY-200417/561
Technicolor					
Tc7200 Firmware NA					
Gain Information	03-04-2017	5	Technicolor TC7200 with firmware STD6.01.12 could allow remote attackers to obtain sensitive information. **CVE ID: CVE-2014-1677**	NA	O-TEC-TC720-200417/562
XEN					
XEN Xen is an open source virtual machine monitor for x86-compatible computers.					
NA	04-04-2017	7.2	An issue (known as XSA-212) was discovered in Xen, with fixes available for 4.8.x, 4.7.x, 4.6.x, 4.5.x, and 4.4.x. The earlier XSA-29 fix introduced an insufficient check on XENMEM_exchange input, allowing the caller to drive hypervisor memory accesses outside of the guest provided input/output arrays. **CVE ID: CVE-2017-7228**	http://openwall.com/lists/oss-security/2017/04/04/3	O-XEN-XEN-200417/563
Zyxel					
Emg2926 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

NA					
Execute Code	06-04-2017	9	A command injection vulnerability was discovered on the Zyxel EMG2926 home router with firmware V1.00(AAQT.4)b8. The vulnerability is located in the diagnostic tools, specifically the nslookup function. A malicious user may exploit numerous vectors to execute arbitrary commands on the router, such as the ping_ip parameter to the expert/maintenance/diagnostic/nslookup URI. **CVE ID: CVE-2017-6884**	https://www.exploit-db.com/exploits/41782/	O-ZYX-EMG29-200417/564