National Critical Information Infrastructure Protection Centre

CVE Report

16-30 April 2017 **Vol. 04 No. 07**

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Aescrypt Project					
Aescrypt Aescrypt is a simple and opinionated AES encrypt / decrypt Ruby gem that just works.					
NA	19-04-2017	5	The aescrypt gem 1.0.0 for Ruby does not randomize the CBC IV for use with the AESCrypt.encrypt and AESCrypt.decrypt functions, which allows attackers to defeat cryptographic protection mechanisms via a chosen plaintext attack. **CVE ID: CVE-2013-7463**	NA	A-AES-AESCR-010517/01
Apache					
Batik Batik is a Java-based toolkit for applications or applets that want to use images in the Scalable Vector Graphics (SVG) format for various purposes, such as display, generation or manipulation.					
DoS	18-04-2017	7.9	In Apache Batik before 1.9, files lying on the filesystem of the server which uses batik can be revealed to arbitrary users who send maliciously formed SVG files. The file types that can be shown depend on the user context in which the exploitable application is running. If the user is root a full compromise of the server - including confidential or sensitive files - would be possible. XXE can also be used to attack the availability of the server via denial of service as the references within a xml document can trivially trigger an amplification attack. **CVE ID: CVE-2017-5662**	https://xmlgraphics.apache.org/security.html	A-APA-BATIK-010517/02
Apache					
CXF Apache CXF is an open source services framework. CXF helps you build and develop services using					

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

frontend programming APIs, like JAX-WS and JAX-RS.					
NA	18-04-2017	5	Apache CXF's STSClient before 3.1.11 and 3.0.13 uses a flawed way of caching tokens that are associated with delegation tokens, which means that an attacker could craft a token which would return an identifer corresponding to a cached token for another user. **CVE ID: CVE-2017-5656**	http://cxf.apache.org/security-advisories.data/CVE-2017-5656.txt.asc?version=1&modificationDate=1492515113282&api=v2	A-APA-CXF-010517/03
CXF Apache CXF is an open source services framework. CXF helps you build and develop services using frontend programming APIs, like JAX-WS and JAX-RS.					
NA	18-04-2017	5	JAX-RS XML Security streaming clients in Apache CXF before 3.1.11 and 3.0.13 do not validate that the service response was signed or encrypted, which allows remote attackers to spoof servers. **CVE ID: CVE-2017-5653**	http://cxf.apache.org/security-advisories.data/CVE-2017-5653.txt.asc?version=1&modificationDate=1492515074710&api=v2	A-APA-CXF-010517/04
Apache					
Formatting Objects Processor Formatting Objects Processor is a Java application that converts XSL Formatting Objects (XSL-FO) files to PDF or other printable formats					
DoS	18-04-2017	7.9	In Apache FOP before 2.2, files lying on the file system of the server which uses FOP can be revealed to arbitrary users who send maliciously formed SVG files. The file types that can be shown depend on the user context in which the exploitable application is running. If the user is root a full compromise of the server - including confidential or sensitive files - would be possible. XXE can also be used to attack the availability of the server via denial of service as the	https://xmlgraphics.apache.org/security.html	A-APA-FORMA-010517/05

			references within a xml document can trivially trigger an amplification attack. **CVE ID: CVE-2017-5661**		
Log4j log4j is a reliable, fast and flexible logging framework (APIs) written in Java, which is distributed under the Apache Software License.					
Execute Code	17-04-2017	7.5	In Apache Log4j 2.x before 2.8.2, when using the TCP socket server or UDP socket server to receive serialized log events from another application, a specially crafted binary payload can be sent that, when deserialized, can execute arbitrary code. **CVE ID: CVE-2017-5645**	https://issues.apache.org/jira/browse/LOG4J2-1863	A-APA-LOG4J-010517/06
Tomcat Apache Tomcat, often referred to as Tomcat Server, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF).					
Gain Information	17-04-2017	5	A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C. **CVE ID: CVE-2017-5647**	https://lists.apache.org/thread.html/5796678c5a773c6f3ff57c178ac247d85ceca0dee9190ba48171451a@%3Cusers.tomcat.apache.org%3E	A-APA-TOMCA-010517/07
NA	17-04-2017	5	In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the handling of an HTTP/2 GOAWAY frame for a connection did not close streams associated with that connection that were currently waiting for a WINDOW_UPDATE before allowing the application to write more data. These waiting	NA	A-APA-TOMCA-010517/08

			streams each consumed a thread. A malicious client could therefore construct a series of HTTP/2 requests that would consume all available processing threads. **CVE ID: CVE-2017-5650**		
NA	17-04-2017	7.5	In Apache Tomcat 9.0.0.M1 to 9.0.0.M18 and 8.5.0 to 8.5.12, the refactoring of the HTTP connectors introduced a regression in the send file processing. If the send file processing completed quickly, it was possible for the Processor to be added to the processor cache twice. This could result in the same Processor being used for multiple requests which in turn could lead to unexpected errors and/or response mix-up. **CVE ID: CVE-2017-5651**	https://bz.apache.org/bugzilla/show_bug.cgi?id=60918	A-APA-TOMCA-010517/09
NA	17-04-2017	6.4	While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application. **CVE ID: CVE-2017-5648**	NA	A-APA-TOMCA-010517/10
Traffic Server Apache Traffic Server software is a fast, scalable and extensible HTTP/1.1 compliant caching proxy server					
NA	17-04-2017	7.8	Apache Traffic Server 6.0.0 to 6.2.0 are affected by an HPACK Bomb Attack. **CVE ID: CVE-2016-5396**	https://issues.apache.org/jira/browse/TS-5019	A-APA-TRAFF-010517/11
NA	17-04-2017	5	Apache Traffic Server before 6.2.1 generates a coredump when there	https://issues.apache.org/	A-APA-TRAFF-

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

			is a mismatch between content length and chunked encoding. **CVE ID: CVE-2017-5659**	jira/browse/TS-4819	010517/12
Apple					
Quicktime QuickTime is an extensible multimedia framework developed by Apple Inc., capable of handling various formats of digital video, picture, sound, panoramic images, and interactivity.					
Execute Code; Overflow	24-04-2017	7.5	Buffer overflow in QuickTime before 7.7.1 for Windows allows remote attackers to execute arbitrary code. **CVE ID: CVE-2011-3428**	https://support.apple.com/en-us/HT5016	A-APP-QUICK-010517/13
Safari Safari is a web browser developed by Apple based on the WebKit engine.					
DoS; Execute Code; Overflow	24-04-2017	6.8	WebKit, as used in Safari 5.0.6, allows remote attackers to cause a denial of service (process crash) or arbitrary code execution. **CVE ID: CVE-2011-3438**	http://support.apple.com/kb/HT4808	A-APP-SAFAR-010517/14
ARM					
Mbed Tls mbed TLS (previously PolarSSL) is an implementation of the TLS and SSL protocols and the respective cryptographic algorithms and support code required.					
Execute Code	20-04-2017	6.8	An exploitable free of a stack pointer vulnerability exists in the x509 certificate parsing code of ARM mbed TLS before 1.3.19, 2.x before 2.1.7, and 2.4.x before 2.4.2. A specially crafted x509 certificate, when parsed by mbed TLS library, can cause an invalid free of a stack pointer leading to a potential remote code execution. In order to exploit this vulnerability, an attacker can act as either a client or a server on a network to deliver malicious x509 certificates to vulnerable applications. **CVE ID: CVE-2017-2784**	https://tls.mbed.org/tech-updates/security-advisories/mbedtls-security-advisory-2017-01	A-ARM-MBED -010517/15
Artifex					
Ghostscript Ghostscript is a suite of software based on an interpreter for Adobe Systems' PostScript and Portable Document Format (PDF) page description languages.					

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

DoS; Overflow	19-04-2017	6.8	Integer overflow in the mark_curve function in Artifex Ghostscript 9.21 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via a crafted PostScript document. **CVE ID: CVE-2017-7948**	https://bugs.ghostscript.com/show_bug.cgi?id=697762	A-ART-GHOST-010517/16
Jbig2dec jbig2dec is a decoder implementation of the JBIG2 image compression format.					
DoS Overflow	19-04-2017	5.8	Artifex jbig2dec 0.13 allows out-of-bounds writes and reads because of an integer overflow in the jbig2_image_compose function in jbig2_image.c during operations on a crafted .jb2 file, leading to a denial of service (application crash) or disclosure of sensitive information from process memory. **CVE ID: CVE-2017-7976**	https://bugs.ghostscript.com/show_bug.cgi?id=697683	A-ART-JBIG2-010517/17
DoS Overflow	16-04-2017	5.8	Artifex jbig2dec 0.13 has a heap-based buffer over-read leading to denial of service (application crash) or disclosure of sensitive information from process memory, because of an integer overflow in the jbig2_decode_symbol_dict function in jbig2_symbol_dict.c in libjbig2dec.a during operation on a crafted .jb2 file. **CVE ID: CVE-2017-7885**	https://bugs.ghostscript.com/show_bug.cgi?id=697703	A-ART-JBIG2-010517/18
DoS Execute Code Overflow	19-04-2017	6.8	Artifex jbig2dec 0.13, as used in Ghostscript, allows out-of-bounds writes because of an integer overflow in the jbig2_build_huffman_table function in jbig2_huffman.c during operations on a crafted JBIG2 file, leading to a denial of service (application crash) or possibly execution of arbitrary code. **CVE ID: CVE-2017-7975**	https://bugs.ghostscript.com/show_bug.cgi?id=697693	A-ART-JBIG2-010517/19
BRO					

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

BRO NA					
DoS; Overflow	24-04-2017	5	analyzer/protocol/dnp3/DNP3.cc in Bro before 2.3.2 does not properly handle zero values of a packet length, which allows remote attackers to cause a denial of service (buffer overflow or buffer over-read if NDEBUG; otherwise assertion failure) via a crafted DNP3 packet. **CVE ID: CVE-2015-1521**	https://github.com/bro/bro/commit/6cedd67c381ff22fde653adf02ee31caf66c81a0	A-BRO-BRO-010517/20
DoS; Overflow	24-04-2017	5	analyzer/protocol/dnp3/DNP3.cc in Bro before 2.3.2 does not reject certain non-zero values of a packet length, which allows remote attackers to cause a denial of service (buffer overflow or buffer over-read) via a crafted DNP3 packet. **CVE ID: CVE-2015-1522**	https://github.com/bro/bro/commit/6cedd67c381ff22fde653adf02ee31caf66c81a0	A-BRO-BRO-010517/21
Browserweb Inc					
Whizz WHIZZ is a WordPress Plugin developed by Browserweb Inc.					
CSRF	24-04-2017	5.8	There is CSRF in the WHIZZ plugin before 1.1.1 for WordPress, allowing attackers to delete any WordPress users and change the plugin's status via a GET request. **CVE ID: CVE-2017-8099**	NA	A-BRO-WHIZZ-010517/22
Capnproto					
Capnproto Cap'n Proto is an insanely fast data interchange format and capability-based RPC system.					
Overflow	17-04-2017	5	Sandstorm Cap'n Proto before 0.5.3.1 allows remote crashes related to a compiler optimization. A remote attacker can trigger a segfault in a 32-bit libcapnp application because Cap'n Proto relies on pointer arithmetic calculations that overflow. An example compiler with optimization that elides a bounds check in such calculations is Apple LLVM version 8.1.0 (clang-802.0.41). The attack vector is a crafted far pointer within	https://github.com/sandstorm-io/capnproto/blob/master/security-advisories/17-04-2017-0-apple-clang-elides-	A-CAP-CAPNP-010517/23

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

			a message. **CVE ID: CVE-2017-7892**	bounds-check.md	
Cisco					
Adaptive Security Appliance Software; Findit Network Probe; Firepower Management Center; Firepower System Software; Integrated Management Controller Supervisor; Prime Network Registrar; Unified Communications Manager Cisco Systems, Inc. (known as Cisco) is an 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.					
DoS	20-04-2017	5.8	A vulnerability in the DNS code of Cisco ASA Software could allow an unauthenticated, remote attacker to cause an affected device to reload or corrupt the information present in the device's local DNS cache. The vulnerability is due to a flaw in handling crafted DNS response messages. An attacker could exploit this vulnerability by triggering a DNS request from the Cisco ASA Software and replying with a crafted response. A successful exploit could cause the device to reload, resulting in a denial of service (DoS) condition or corruption of the local DNS cache information. Note: Only traffic directed to the affected device can be used to exploit this vulnerability. This vulnerability affects Cisco ASA Software configured in routed or transparent firewall mode and single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. This vulnerability affects Cisco ASA Software running on the following products: Cisco ASA 1000V Cloud Firewall, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco ASA 5500-X Series Next-Generation Firewalls, Cisco ASA Services	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-dns	A-CIS-ADAPT-010517/24

			Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Cisco Adaptive Security Virtual Appliance (ASAv), Cisco Firepower 9300 ASA Security Module, Cisco ISA 3000 Industrial Security Appliance. Fixed versions: 9.1(7.12) 9.2(4.18) 9.4(3.12) 9.5(3.2) 9.6(2.2). Cisco Bug IDs: CSCvb40898. **CVE ID: CVE-2017-6607**		
NA	20-04-2017	6.8	A vulnerability in the Internet Key Exchange Version 1 (IKEv1) XAUTH code of Cisco ASA Software could allow an authenticated, remote attacker to cause a reload of an affected system. The vulnerability is due to insufficient validation of the IKEv1 XAUTH parameters passed during an IKEv1 negotiation. An attacker could exploit this vulnerability by sending crafted parameters. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability only affects systems configured in routed firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 or IPv6 traffic. A valid IKEv1 Phase 1 needs to be established to exploit this vulnerability, which means that an attacker would need to have knowledge of a pre-shared key or have a valid certificate for phase 1 authentication. This vulnerability affects Cisco ASA Software running on the following products: Cisco ASA 1000V Cloud Firewall, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco ASA 5500-X Series Next-Generation Firewalls, Cisco ASA Services Module for Cisco Catalyst 6500	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-xauth	A-CIS-ADAPT-010517/25

			Series Switches and Cisco 7600 Series Routers, Cisco Adaptive Security Virtual Appliance (ASAv), Cisco ASA for Firepower 9300 Series, Cisco ISA 3000 Industrial Security Appliance. Fixed versions: 9.1(7.7) 9.2(4.11) 9.4(4) 9.5(3) 9.6(1.5). Cisco Bug IDs: CSCuz11685. **CVE ID: CVE-2017-6610**		
NA	20-04-2017	6.8	A vulnerability in the IPsec code of Cisco ASA Software could allow an authenticated, remote attacker to cause a reload of the affected system. The vulnerability is due to improper parsing of malformed IPsec packets. An attacker could exploit this vulnerability by sending malformed IPsec packets to the affected system. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed firewall mode only and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. An attacker needs to establish a valid IPsec tunnel before exploiting this vulnerability. This vulnerability affects Cisco ASA Software running on the following products: Cisco ASA 1000V Cloud Firewall, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco ASA 5500-X Series Next-Generation Firewalls, Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Cisco Adaptive Security Virtual Appliance (ASAv), Cisco Firepower 9300 ASA Security Module, Cisco ISA 3000 Industrial Security Appliance. Fixed versions: 9.1(7.8) 9.2(4.15) 9.4(4) 9.5(3.2)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-ipsec	A-CIS-ADAPT-010517/26

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

			9.6(2). Cisco Bug IDs: CSCun16158. **CVE ID: CVE-2017-6609**		
NA	20-04-2017	7.8	A vulnerability in the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) code of Cisco ASA Software could allow an unauthenticated, remote attacker to cause a reload of the affected system. The vulnerability is due to improper parsing of crafted SSL or TLS packets. An attacker could exploit this vulnerability by sending a crafted packet to the affected system. Note: Only traffic directed to the affected system can be used to exploit this vulnerability. This vulnerability affects systems configured in routed and transparent firewall mode and in single or multiple context mode. This vulnerability can be triggered by IPv4 and IPv6 traffic. A valid SSL or TLS session is needed to exploit this vulnerability. This vulnerability affects Cisco ASA Software running on the following products: Cisco ASA 1000V Cloud Firewall, Cisco ASA 5500 Series Adaptive Security Appliances, Cisco ASA 5500-X Series Next-Generation Firewalls, Cisco ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, Cisco Adaptive Security Virtual Appliance (ASAv), Cisco Firepower 9300 ASA Security Module, Cisco ISA 3000 Industrial Security Appliance. Fixed versions: 8.4(7.31) 9.0(4.39) 9.1(7) 9.2(4.6) 9.3(3.8) 9.4(2) 9.5(2). Cisco Bug IDs: CSCuv48243. **CVE ID: CVE-2017-6608**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-asa-tls	A-CIS-ADAPT-010517/27
Gain Information	20-04-2017	6.8	A vulnerability in the file-download feature of the web user interface for Cisco FindIT Network Probe Software 1.0.0 could allow an	https://tools.cisco.com/security/center/conte	A-CIS-FINDI-010517/28

			authenticated, remote attacker to download and view any system file by using the affected software. The vulnerability is due to the absence of role-based access control (RBAC) for file-download requests that are sent to the affected software. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker to download and view any system file by using the affected software. Cisco Bug IDs: CSCvd11628. **CVE ID: CVE-2017-6614**	nt/CiscoSecurityAdvisory/cisco-sa-20170419-findit	
DoS Bypass	20-04-2017	5	A vulnerability in the detection engine parsing of Pragmatic General Multicast (PGM) protocol packets for Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition due to the Snort process unexpectedly restarting. The vulnerability is due to improper input validation of the fields in the PGM protocol packet. An attacker could exploit this vulnerability by sending a crafted PGM packet to the detection engine on the targeted device. An exploit could allow the attacker to cause a DoS condition if the Snort process restarts and traffic inspection is bypassed or traffic is dropped. This vulnerability affects Cisco Firepower System Software that has one or more file action policies configured and is running on any of the following Cisco products: Adaptive Security Appliance (ASA) 5500-X Series with FirePOWER Services; Adaptive Security Appliance (ASA) 5500-X Series Next-Generation Firewalls;	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-fpsnort	A-CIS-FIREP-010517/29

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

			Advanced Malware Protection (AMP) for Networks, 7000 Series Appliances; Advanced Malware Protection (AMP) for Networks, 8000 Series Appliances; Firepower 4100 Series Security Appliances; FirePOWER 7000 Series Appliances; FirePOWER 8000 Series Appliances; Firepower 9300 Series Security Appliances; FirePOWER Threat Defense for Integrated Services Routers (ISRs); Industrial Security Appliance 3000; Sourcefire 3D System Appliances; Virtual Next-Generation Intrusion Prevention System (NGIPSv) for VMware. Fixed versions: 5.4.0.10 5.4.1.9 6.0.1.3 6.1.0 6.2.0. Cisco Bug IDs: CSCuz00876. **CVE ID: CVE-2016-6368**		
Execute Code	20-04-2017	9	A vulnerability in the web-based GUI of Cisco Integrated Management Controller (IMC) 3.0(1c) could allow an authenticated, remote attacker to execute arbitrary code on an affected system. The vulnerability exists because the affected software does not sufficiently sanitize specific values that are received as part of a user-supplied HTTP request. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected software. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the user on the affected system. Cisco Bug IDs: CSCvd14578. **CVE ID: CVE-2017-6616**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-cimc3	A-CIS-INTEG-010517/30
Execute Code	20-04-2017	9	A vulnerability in the web-based GUI of Cisco Integrated Management Controller (IMC) 3.0(1c) could allow an authenticated, remote attacker to	https://tools.cisco.com/security/center/content/CiscoSec	A-CIS-INTEG-010517/31

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 arbitrary commands on an affected system. The vulnerability exists because the affected software does not sufficiently sanitize user-supplied HTTP input. An attacker could exploit this vulnerability by sending an HTTP POST request that contains crafted, deserialized user data to the affected software. A successful exploit could allow the attacker to execute arbitrary commands with root-level privileges on the affected system, which the attacker could use to conduct further attacks. Cisco Bug IDs: CSCvd14591. **CVE ID: CVE-2017-6619**	urityAdvisory/cisco-sa-20170419-cimc	
DoS	20-04-2017	5	A vulnerability in the DNS input packet processor for Cisco Prime Network Registrar could allow an unauthenticated, remote attacker to cause the DNS process to momentarily restart, which could lead to a partial denial of service (DoS) condition on the affected system. The vulnerability is due to incomplete DNS packet header validation when the packet is received by the application. An attacker could exploit this vulnerability by sending a malformed DNS packet to the application. An exploit could allow the attacker to cause the DNS process to restart, which could lead to a DoS condition. This vulnerability affects Cisco Prime Network Registrar on all software versions prior to 8.3.5. Cisco Bug IDs: CSCvb55412. **CVE ID: CVE-2017-6613**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-prime-dns	A-CIS-PRIME-010517/32
DoS; Overflow	20-04-2017	7.8	A vulnerability in the Session Initiation Protocol (SIP) UDP throttling process of Cisco Unified Communications Manager (Cisco	https://tools.cisco.com/security/center/conte	A-CIS-UNIFI-010517/33

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

			Unified CM) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to insufficient rate limiting protection. An attacker could exploit this vulnerability by sending the affected device a high rate of SIP messages. An exploit could allow the attacker to cause the device to reload unexpectedly. The device and services will restart automatically. This vulnerability affects Cisco Unified Communications Manager (CallManager) releases prior to the first fixed release; the following list indicates the first minor release that includes the fix for this vulnerability: 10.5.2.14900-16 11.0.1.23900-5 11.5.1.12900-2. Cisco Bug IDs: CSCuz72455. **CVE ID: CVE-2017-3808**	nt/CiscoSecurityAdvisory/cisco-sa-20170419-ucm	
Cloud Foundry					
Cf-release NA					
NA	20-04-2017	6.8	The Cloud Controller in Cloud Foundry cf-release versions prior to v255 allows authenticated developer users to exceed memory and disk quotas for tasks. **CVE ID: CVE-2017-4969**	https://www.cloudfoundry.org/CVE-2017-4969/	A-CLO-CF-RE-010517/34
Cs-cart					
Cs-cart NA					
Execute Code	20-04-2017	6.5	Twigmo bundled with CS-Cart 4.3.9 and earlier and Twigmo bundled with CS-Cart Multi-Vendor 4.3.9 and earlier allow remote authenticated users to execute arbitrary PHP code on the servers. **CVE ID: CVE-2016-4862**	http://tips.cs-cart.jp/fix-twigmo-vulnerability-20160914.html	A-CS-CSCA-010517/35
Cybozu					

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

Garoon; Office Cybozu, Inc. is a Tokyo-based software company that provides a web-based groupware known as Cybozu Office, popular in Japan.					
Bypass	20-04-2017	7.5	Cybozu Garoon before 4.2.2 allows remote attackers to bypass login authentication via vectors related to API use. **CVE ID: CVE-2016-1219**	https://support.cybozu.com/ja-jp/article/9408	A-CYB-GAROO-010517/36
Sql	20-04-2017	6.5	SQL injection vulnerability in Cybozu Garoon before 4.2.2. **CVE ID: CVE-2016-1218**	https://support.cybozu.com/ja-jp/article/9414	A-CYB-GAROO-010517/37
NA	20-04-2017	5.8	The "Scheduler" function in Cybozu Garoon before 4.2.2 allows remote attackers to redirect users to arbitrary websites. **CVE ID: CVE-2016-1213**	https://support.cybozu.com/ja-jp/article/9221	A-CYB-GAROO-010517/38
DoS	17-04-2017	6.8	Cybozu Office 9.0.0 through 10.4.0 allows remote attackers to cause a denial of service. **CVE ID: CVE-2016-4871**	https://support.cybozu.com/ja-jp/article/9426	A-CYB-OFFIC-010517/39
Cygwin					
Cygwin NA					
Gain Privileges	21-04-2017	7.5	Cygwin before 2.5.0 does not properly handle updating permissions when changing users, which allows attackers to gain privileges. **CVE ID: CVE-2016-3067**	https://sourceware.org/git/?p=newlib-cygwin.git;a=commit;h=205862ed08649df8f50b926a2c58c963f571b044	A-CYG-CYGWI-010517/40
Drupal					
Drupal Drupal is a scalable, open platform for web content management and digital experiences.					
Bypass	19-04-2017	6	Drupal 8 before 8.2.8 and 8.3 before 8.3.1 allows critical access bypass by authenticated users if the RESTful Web Services (rest) module	https://www.drupal.org/SA-CORE-2017-002	A-DRU-DRUPA-010517/41

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

			is enabled and the site allows PATCH requests. **CVE ID: CVE-2017-6919**		
Exponentcms					
Exponent Cms Exponent CMS is an Open Source Content Management System, based on PHP, MySQL and the Exponent Framework.					
Sql	21-04-2017	7.5	Exponent CMS 2.4.1 and earlier has SQL injection via a base64 serialized API key (apikey parameter) in the api function of framework/modules/eaas/controllers/eaasController.php. **CVE ID: CVE-2017-7991**	NA	A-EXP-EXPON-010517/42
Extplorer					
Extplorer NA					
Directory Traversal	24-04-2017	6.8	Directory traversal vulnerability in unzip/extract feature in eXtplorer 2.1.9 allows remote attackers to execute arbitrary files via a .. (dot dot) in an archive file. **CVE ID: CVE-2016-4313**	NA	A-EXT-EXTPL-010517/43
Freetype					
Freetype NA					
Overflow	24-04-2017	7.5	FreeType 2 before 2017-03-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_decoder_parse_charstrings function in psaux/t1decode.c. **CVE ID: CVE-2017-8105**	NA	A-FRE-FREET-010517/44
Gnome					
Libcroco NA					
DoS; Overflow	19-04-2017	6.8	** DISPUTED ** The cr_tknzr_parse_rgb function in cr-tknzr.c in libcroco 0.6.11 and 0.6.12 has an "outside the range of representable values of type long" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified	NA	A-GNO-LIBCR-010517/45

			other impact via a crafted CSS file. NOTE: third-party analysis reports "This is not a security issue in my view. The conversion surely is truncating the double into a long value, but there is no impact as the value is one of the RGB components." **CVE ID: CVE-2017-7961**		
Google					
Chrome Google Chrome is a freeware web browser developed by Google.					
NA	24-04-2017	6.8	A use after free in ANGLE in Google Chrome prior to 57.0.2987.98 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID: CVE-2017-5031**	https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html	A-GOO-CHROM-010517/46
NA	24-04-2017	6.8	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. **CVE ID: CVE-2017-5034**	https://crbug.com/678461	A-GOO-CHROM-010517/47
NA	24-04-2017	6.8	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file. **CVE ID: CVE-2017-5036**	https://crbug.com/691371	A-GOO-CHROM-010517/48
NA	24-04-2017	6.8	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID: CVE-2017-5039**	https://crbug.com/679649	A-GOO-CHROM-010517/49
Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in	https://crb	A-GOO-

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

			Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5051**	ug.com/679641	CHROM-010517/50
Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5050**	https://crbug.com/679645	A-GOO-CHROM-010517/51
Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5049**	https://crbug.com/679646	A-GOO-CHROM-010517/52
Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5048**	https://crbug.com/679647	A-GOO-CHROM-010517/53
Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5047**	https://crbug.com/679653	A-GOO-CHROM-010517/54

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

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

Overflow	24-04-2017	6.8	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer. **CVE ID: CVE-2017-5037**	https://crbug.com/679640	A-GOO-CHROM-010517/55
NA	24-04-2017	6.8	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension. **CVE ID: CVE-2017-5043**	https://crbug.com/683523	A-GOO-CHROM-010517/56
NA	24-04-2017	6.8	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension. **CVE ID: CVE-2017-5038**	https://crbug.com/695476	A-GOO-CHROM-010517/57
NA	24-04-2017	6.8	Google Chrome prior to 57.0.2987.98 for Windows and Mac had a race condition, which could cause Chrome to display incorrect certificate information for a site. **CVE ID: CVE-2017-5035**	https://crbug.com/688425	A-GOO-CHROM-010517/58
Overflow	24-04-2017	6.8	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. **CVE ID: CVE-2017-5044**	https://crbug.com/688987	A-GOO-CHROM-010517/59
Execute Code Overflow	24-04-2017	6.8	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a	https://crbug.com/682194	A-GOO-CHROM-010517/60

			crafted HTML page. **CVE ID: CVE-2017-5030**		
NA	24-04-2017	6.8	PDFium in Google Chrome prior to 57.0.2987.98 for Windows could be made to increment off the end of a buffer, which allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID: CVE-2017-5032**	https://crbug.com/668724	A-GOO-CHROM-010517/61
Bypass; Gain Information	21-04-2017	5	Skia, as used in Google Chrome before 50.0.2661.94, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information. **CVE ID: CVE-2016-5168**	https://chromereleases.googleblog.com/2016/04/stable-channel-update_28.html	A-GOO-CHROM-010517/62
Google;Xmlsoft					
Chrome/Libxslt Google Chrome is a freeware web browser developed by Google/ NA					
Overflow	24-04-2017	6.8	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. **CVE ID: CVE-2017-5029**	https://chromereleases.googleblog.com/2017/03/stable-channel-update-for-desktop.html	A-GOO-CHROM-010517/63
Grandstream					
Wave NA					
Gain Information	21-04-2017	6.8	The auto-provisioning mechanism in the Grandstream Wave app 1.0.1.26 and earlier for Android and Grandstream Video IP phones allows man-in-the-middle attackers to spoof provisioning data and consequently modify device functionality, obtain	NA	A-GRA-WAVE-010517/64

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

			sensitive information from system logs, and have unspecified other impact by leveraging failure to use an HTTPS session for downloading configuration files from http://fm.grandstream.com/gs/. **CVE ID: CVE-2016-1518**		
Execute Code	21-04-2017	6.8	The Grandstream Wave app 1.0.1.26 and earlier for Android does not use HTTPS when retrieving update information, which might allow man-in-the-middle attackers to execute arbitrary code via a crafted application. **CVE ID: CVE-2016-1520**		A-GRA-WAVE-010517/65
Hancom					
Hancom Office 2014 NA					
Execute Code; Overflow	20-04-2017	6.8	Multiple heap-based buffer overflows in the (1) CBookBase::SetDefTableStyle and (2) CBookBase::SetDefPivotStyle functions in Hancom Office 2014 VP allow remote attackers to execute arbitrary code via a crafted Hangul Hcell Document (.cell) file. **CVE ID: CVE-2016-4293**	NA	A-HAN-HANCO-010517/66
IBM					
Api Connect; Change And Configuration Management Database; Maximo Asset Management; Maximo Asset Management Essentials; Maximo For Government; Maximo For Life Sciences; Maximo For Nuclear Power; Maximo For Oil And Gas; Maximo For Transportation; Maximo For Utilities; Tivoli Asset Management For It; Tivoli Service Request Manager; Cognos Business Intelligence; Security Guardium; International Business Machines Corporation is an American multinational technology company headquartered in Armonk, New York, United States, with operations in over 170 countries.					

Execute Code	17-04-2017	7.5	IBM API Connect 5.0.6.0 could allow a remote attacker to execute arbitrary commands on the system, caused by improper validation of URLs for the Developer Portal. By crafting a malicious URL, an attacker could exploit this vulnerability to execute arbitrary commands on the system with the privileges of the www-data user. IBM X-Force ID: 122956. **CVE ID: CVE-2017-1161**	http://www.ibm.com/support/docview.wss?uid=swg22000316	A-IBM-API C-010517/67
Execute Code	24-04-2017	6.5	IBM Tivoli IT Asset Management for IT, Tivoli Service Request Manager, and Change and Configuration Management Database 7.1 through 7.1.1.8 and 7.2 and Maximo Asset Management and Maximo Industry Solutions 7.1 through 7.1.1.8, 7.5 before 7.5.0.7 IFIX003, and 7.6 before 7.6.0.0 IFIX002 allow remote authenticated users to execute arbitrary code via unspecified vectors. **CVE ID: CVE-2015-0104**	http://www-01.ibm.com/support/docview.wss?uid=swg21694974	A-IBM-CHANG-010517/68
DoS; Overflow	17-04-2017	5	IBM Cognos TM1 10.1 and 10.2 is vulnerable to a denial of service, caused by a stack-based buffer overflow when parsing packets. A remote attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 114612. **CVE ID: CVE-2016-3036**	http://www.ibm.com/support/docview.wss?uid=swg21999649	A-IBM-COGNO-010517/69
Execute Code	20-04-2017	6.9	IBM Security Guardium 8.2, 9.0, and 10.0 contains a vulnerability that could allow a local attacker with CLI access to inject arbitrary commands which would be executed as root. IBM X-Force ID: 121174. **CVE ID: CVE-2017-1122**	http://www.ibm.com/support/docview.wss?uid=swg21997868	A-IBM-SECUR-010517/70

Imagemagick

Imagemagick

ImageMagick is a software suite to create, edit, compose, or convert bitmap images.

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	20-04-2017	7.1	coders/dds.c in ImageMagick before 6.9.0-4 Beta allows remote attackers to cause a denial of service (CPU consumption) via a crafted DDS file. **CVE ID: CVE-2015-8959**	http://www.imagemagick.org/discourse-server/viewtopic.php?f=3&t=26861	A-IMA-IMAGE-010517/71
Irregex Project					
Irregex NA					
DoS	21-04-2017	5	The backtrack compilation code in the Irregex package (aka IrRegular Expressions) before 0.9.6 for Scheme allows remote attackers to cause a denial of service (memory consumption) via a crafted regular expression with a repeating pattern. **CVE ID: CVE-2016-9954**	https://github.com/ashinn/irregex/commit/a16ffc86eca15fca9e40607d41de3cea9cf868f1	A-IRR-IRREG-010517/72
Juniper					
Northstar Controller Juniper Networks NorthStar Controller is a powerful and flexible traffic-engineering solution that enables granular visibility and control of IP/MPLS flows in large service provider and enterprise networks.					
DoS	24-04-2017	5	A command injection vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow a network-based malicious attacker to cause a denial of service condition. **CVE ID: CVE-2017-2324**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/73
DoS	24-04-2017	5	A denial of service vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow a malicious attacker crafting packets destined to the device to cause a persistent denial of service to the path computation server service. **CVE ID: CVE-2017-2323**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/74
DoS	24-04-2017	7.5	A denial of service vulnerability in Juniper Networks NorthStar Controller Application prior to	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/75

			version 2.1.0 Service Pack 1 may allow an unauthenticated, unprivileged, network-based attacker to cause denials of services to underlying database tables leading to potential information disclosure, modification of system states, and partial to full denial of services relying upon data modified by an attacker. **CVE ID: CVE-2017-2317**		
DoS; Bypass	24-04-2017	7.5	A firewall bypass vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow a network-based malicious attacker to bypass firewall policies, leading to authentication bypass methods, information disclosure, modification of system files, and denials of service. **CVE ID: CVE-2017-2331**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/76
NA	24-04-2017	7.5	A vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow a malicious attacker to compromise the systems confidentiality or integrity without authentication, leading to managed systems being compromised or services being denied to authentic end users and systems as a result. **CVE ID: CVE-2017-2319**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/77
DoS	24-04-2017	10	A vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow an unauthenticated, unprivileged, network-based attacker to cause various denials of services leading to targeted information disclosure, modification of any component of the NorthStar system, including managed systems, and full denial of services to any systems under management which	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/78

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

			NorthStar interacts with using read-only or read-write credentials. **CVE ID: CVE-2017-2320**		
DoS Execute Code	24-04-2017	7.5	A vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow an unauthenticated, unprivileged, network-based attacker to cause various system services partial to full denials of services, modification of system states and files, and potential disclosure of sensitive information which may assist the attacker in further attacks on the system through the use of multiple attack vectors, including man-in-the-middle attacks, file injections, and malicious execution of commands causing out of bound memory conditions leading to other attacks. **CVE ID: CVE-2017-2321**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/79
Gain Information	24-04-2017	6.8	An information disclosure vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow an unprivileged, authenticated, network-based attacker to replicate the underlying Junos OS VM and all data it maintains to their local system for future analysis. **CVE ID: CVE-2017-2326**	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/80
Gain Privileges	24-04-2017	9.3	An insufficient authentication vulnerability in Juniper Networks NorthStar Controller Application prior to version 2.1.0 Service Pack 1 may allow a malicious, network based, unauthenticated attacker to perform privileged actions to gain complete control over the	https://kb.juniper.net/JSA10783	A-JUN-NORTH-010517/81

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

			environment. **CVE ID: CVE-2017-2332**		
Kallithea					
Kallithea NA					
Bypass; CSRF	24-04-2017	6.8	Routes in Kallithea before 0.3.2 allows remote attackers to bypass the CSRF protection by using the GET HTTP request method. **CVE ID: CVE-2016-3691**	http://www.openwall.com/lists/oss-security/2016/05/02/3	A-KAL-KALLI-010517/82
Lenovo					
Lenovo System Update Lenovo System Update is the updater program which runs with Windows (in the background as a service) and automatically starts up when your computer boots.					
Gain Privileges	24-04-2017	6.9	Lenovo System Update (formerly ThinkVantage System Update) before 5.07.0019 allows local users to gain privileges by making a prediction of tvsu_tmp_xxxxxXXXXX account credentials that requires knowledge of the time that this account was created, aka a "temporary administrator account vulnerability." **CVE ID: CVE-2015-8109**	https://support.lenovo.com/us/en/product_security/lsu_privilege	A-LEN-LENOV-010517/83
Gain Privileges	24-04-2017	7.2	Lenovo System Update (formerly ThinkVantage System Update) before 5.07.0019 allows local users to gain privileges by navigating to (1) "Click here to learn more" or (2) "View privacy policy" within the Tvsukernel.exe GUI application in the context of a temporary administrator account, aka a "local privilege escalation vulnerability." **CVE ID: CVE-2015-8110**	https://support.lenovo.com/us/en/product_security/lsu_privilege	A-LEN-LENOV-010517/84
Linecorp					
Line NA					
Execute Code	20-04-2017	6.8	LINE for Windows before 4.8.3 allows man-in-the-middle attackers to execute arbitrary code. **CVE ID: CVE-2016-4850**	https://linecorp.com/ja/security/article/65	A-LIN-LINE-010517/85

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

Lshell Project					
Lshell LShell or Limited Shell is written in python for limiting user for specific set of commands and directories.					
Execute Code	24-04-2017	9	lshell 0.9.16 allows remote authenticated users to break out of a limited shell and execute arbitrary commands. **CVE ID: CVE-2016-6903**	https://github.com/ghantoos/lshell/pull/153/commits/a686f71732a3d0f16df52ef46ab8a49ee0083c68	A-LSH-LSHEL-010517/86
Execute Code	24-04-2017	9	lshell 0.9.16 allows remote authenticated users to break out of a limited shell and execute arbitrary commands. **CVE ID: CVE-2016-6902**	https://github.com/ghantoos/lshell/issues/147	A-LSH-LSHEL-010517/87
Mantisbt					
Mantisbt MantisBT is a popular free web-based bug tracking system.					
NA	16-04-2017	6.5	MantisBT through 2.3.0 allows arbitrary password reset and unauthenticated admin access via an empty confirm_hash value to verify.php. **CVE ID: CVE-2017-7615**	https://mantisbt.org/bugs/view.php?id=22690	A-MAN-MANTI-010517/88
Mediawiki					
Mediawiki MediaWiki is a free software open source wiki package written in PHP, originally for use on Wikipedia.					
Bypass	20-04-2017	5	ApiParse in MediaWiki before 1.23.15, 1.26.x before 1.26.4, and 1.27.x before 1.27.1 allows remote attackers to bypass intended per-title read restrictions via a parse action to api.php. **CVE ID: CVE-2016-6331**	https://phabricator.wikimedia.org/T115333	A-MED-MEDIA-010517/89
Bypass	20-04-2017	5	MediaWiki 1.27.x before 1.27.1 might allow remote attackers to bypass intended session access restrictions by leveraging a call to the UserGetRights function after Session::getAllowedUserRights.	https://phabricator.wikimedia.org/T139670	A-MED-MEDIA-010517/90

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**										

			CVE ID: CVE-2016-6337		
Gain Information	20-04-2017	5	MediaWiki before 1.23.15, 1.26.x before 1.26.4, and 1.27.x before 1.27.1 does not generate head items in the context of a given title, which allows remote attackers to obtain sensitive information via a parse action to api.php. **CVE ID: CVE-2016-6335**	https://phabricator.wikimedia.org/T139570	A-MED-MEDIA-010517/91
Gain Information	20-04-2017	5	MediaWiki before 1.23.15, 1.26.x before 1.26.4, and 1.27.x before 1.27.1, when $wgBlockDisablesLogin is true, might allow remote attackers to obtain sensitive information by leveraging failure to terminate sessions when a user account is blocked. **CVE ID: CVE-2016-6332**	https://phabricator.wikimedia.org/T129738	A-MED-MEDIA-010517/92
Moodle					
Moodle Moodle is a free and open-source software learning management system written in PHP and distributed under the GNU General Public License.					
CSRF	20-04-2017	6.8	Cross-site request forgery (CSRF) vulnerability in markposts.php in Moodle 3.0 through 3.0.3, 2.9 through 2.9.5, 2.8 through 2.8.11, 2.7 through 2.7.13 and earlier allows remote attackers to hijack the authentication of users for requests that marks forum posts as read. **CVE ID: CVE-2016-3734**	https://bugzilla.redhat.com/show_bug.cgi?id=1335933	A-MOO-MOODL-010517/93
Gain Information	20-04-2017	5	Moodle 3.0 through 3.0.3, 2.9 through 2.9.5, and 2.8 through 2.8.11 allows remote attackers to obtain the names of hidden forums and forum discussions. **CVE ID: CVE-2016-3731**	https://bugzilla.redhat.com/show_bug.cgi?id=1335933	A-MOO-MOODL-010517/94
Mor-pah.net					
Dmitry Deepmagic Information Gathering Tool NA					
DoS; Overflow	20-04-2017	7.5	Stack-based buffer overflow in DMitry (Deepmagic Information	NA	A-MOR-DMITR-

			Gathering Tool) version 1.3a (Unix) allows attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long argument. An example threat model is automated execution of DMitry with hostname strings found in local log files. **CVE ID: CVE-2017-7938**		010517/95
Mybb					
Mybb MyBB, formerly MyBBoard and originally MyBulletinBoard, is a free and open source forum software developed by the MyBB Group.					
Directory Traversal	24-04-2017	5	In MyBB before 1.8.11, the smilie module allows Directory Traversal via the pathfolder parameter. **CVE ID: CVE-2017-8104**	NA	A-MYB-MYBB-010517/96
Novell					
Groupwise GroupWise is a messaging and collaboration platform from Novell that supports email, calendaring, personal information management, instant messaging, and document management					
Execute Code; Overflow	20-04-2017	7.5	Integer overflow in the Post Office Agent in Novell GroupWise before 2014 R2 Service Pack 1 Hot Patch 1 might allow remote attackers to execute arbitrary code via a long (1) username or (2) password, which triggers a heap-based buffer overflow. **CVE ID: CVE-2016-5762**	https://www.novell.com/support/kb/doc.php?id=7017975	A-NOV-GROUP-010517/97
Opendaylight					
Opendaylight Hosted by the Linux Foundation, OpenDaylight Project (ODL) is an open source SDN project aimed at enhancing software-defined networking (SDN) by offering a community-led and industry-supported framework for the OpenDaylight Controller, which has been renamed the OpenDaylight Platform.					
DoS	24-04-2017	5	Denial of Service attack when the switch rejects to receive packets from the controller. Component: This vulnerability affects OpenDaylight odl-l2switch-switch, which is the feature responsible for the OpenFlow communication. Version: OpenDaylight versions 3.3 and 4.0 are affected by this flaw.	https://aaltodoc.aalto.fi/bitstream/handle/123456789/21584/master_Bidaj_Andi_2016.pdf	A-OPE-OPEND-010517/98

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

			Java version is openjdk version 1.8.0_91. **CVE ID: CVE-2017-1000357**		
NA	24-04-2017	5	DOMRpcImplementationNotAvailableException when sending Port-Status packets to OpenDaylight. Controller launches exceptions and consumes more CPU resources. Component: OpenDaylight is vulnerable to this flaw. Version: The tested versions are OpenDaylight 3.3 and 4.0. **CVE ID: CVE-2017-1000361**	https://aaltodoc.aalto.fi/bitstream/handle/123456789/21584/master_Bidaj_Andi_2016.pdf	A-OPE-OPEND-010517/99
NA	24-04-2017	5	Java out of memory error and significant increase in resource consumption. Component: OpenDaylight odl-mdsal-xsql is vulnerable to this flaw. Version: The tested versions are OpenDaylight 3.3 and 4.0. **CVE ID: CVE-2017-1000359**	https://aaltodoc.aalto.fi/bitstream/handle/123456789/21584/master_Bidaj_Andi_2016.pdf	A-OPE-OPEND-010517/100
NA	24-04-2017	5	StreamCorruptedException and NullPointerException in OpenDaylight odl-mdsal-xsql. Controller launches exceptions in the console. Component: OpenDaylight odl-mdsal-xsql is vulnerable to this flaw. Version: The tested versions are OpenDaylight 3.3 and 4.0. **CVE ID: CVE-2017-1000360**	https://aaltodoc.aalto.fi/bitstream/handle/123456789/21584/master_Bidaj_Andi_2016.pdf	A-OPE-OPEND-010517/101
Openmrs					
Openmrs Module Reporting NA					
XSS; CSRF	20-04-2017	6.8	The Reporting Module 1.12.0 for OpenMRS allows CSRF attacks with resultant XSS, in which administrative authentication is hijacked to insert JavaScript into a name field in webapp/reports/manageReports.jsp. **CVE ID: CVE-2017-7990**	NA	A-OPE-OPENM-010517/102
Opentext					

Documentum Content Server Documentum Content Server (core product) Platform that manages content in a repository consisting of three parts: a content server, a relational database, and a place to store files. Items in the repository are stored as an object.					
NA	20-04-2017	9	OpenText Documentum Content Server allows superuser access via sys_obj_save or save of a crafted object, followed by an unauthorized "UPDATE dm_dbo.dm_user_s SET user_privileges=16" command, aka an "RPC save-commands" attack. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4532. **CVE ID: CVE-2017-7220**	NA	A-OPE-DOCUM-010517/103
Opera					
Opera Browser; Opera Mini NA					
NA	20-04-2017	5.8	Opera Mini 13 and Opera Stable 36 allow remote attackers to spoof the displayed URL via a crafted HTML document, related to the about:blank URL. **CVE ID: CVE-2016-4075**	NA	A-OPE-OPERA-010517/104
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	19-04-2017	5	** DISPUTED ** The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's	https://bugs.php.net/bug.php?id=74308	A-PHP-PHP-010517/105

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

			OOM behavior." **CVE ID: CVE-2017-7963**		
DoS; Execute Code	21-04-2017	6.8	The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive. **CVE ID: CVE-2016-5399**	https://bugzilla.redhat.com/show_bug.cgi?id=1358395	A-PHP-PHP-010517/106
Quickheal					
Total Security NA					
DoS; Overflow	20-04-2017	5	The webssx.sys driver in QuickHeal 16.00 allows remote attackers to cause a denial of service. **CVE ID: CVE-2015-8285**	NA	A-QUI-TOTAL-010517/107
Redhat					
Cloudforms Management Engine; Jboss Bpm Suite;Jboss Enterprise Brms Platform; Openshift NA					
Gain Information	21-04-2017	5	Padding oracle flaw in CloudForms Management Engine (aka CFME) 5 allows remote attackers to obtain sensitive cleartext information. **CVE ID: CVE-2016-3702**	https://bugzilla.redhat.com/show_bug.cgi?id=1330179	A-RED-CLOUD-010517/108
CSRF	20-04-2017	6.8	Cross-site request forgery (CSRF) vulnerability in Red Hat JBoss BRMS and BPMS 6 allows remote attackers to hijack the authentication of users for requests that modify instances via a crafted web page. **CVE ID: CVE-2016-5401**	https://bugzilla.redhat.com/show_bug.cgi?id=1357731	A-RED-JBOSS-010517/109
Gain Information	20-04-2017	5	Red Hat OpenShift Enterprise 2 does not include the HTTPOnly flag in a Set-Cookie header for the	https://bugzilla.redhat.com/show_	A-RED-OPENS-010517/110

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

			GEARID cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to the cookies. **CVE ID: CVE-2016-5409**	bug.cgi?id=1366461	
S9Y					
Serendipity NA					
CSRF	24-04-2017	6.8	There is CSRF in Serendipity 2.0.5, allowing attackers to install any themes via a GET request. **CVE ID: CVE-2017-8101**	NA	A-S9Y-SEREN-010517/111
Schneider Electric					
Wonderware Intouch Access Anywhere 2014 NA					
CSRF	20-04-2017	6.8	A Cross-Site Request Forgery issue was discovered in Schneider Electric Wonderware InTouch Access Anywhere, version 11.5.2 and prior. The client request may be forged from a different site. This will allow an external site to access internal RDP systems on behalf of the currently logged in user. **CVE ID: CVE-2017-5156**	NA	A-SCH-WONDE-010517/112
Gain Information	20-04-2017	5	An Information Exposure issue was discovered in Schneider Electric Wonderware InTouch Access Anywhere, version 11.5.2 and prior. Credentials may be exposed to external systems via specific URL parameters, as arbitrary destination addresses may be specified. **CVE ID: CVE-2017-5158**	NA	A-SCH-WONDE-010517/113
Securebrain					
Phishwall Client NA					
NA	21-04-2017	9.3	Untrusted search path vulnerability in the installer of PhishWall Client Internet Explorer before 3.7.8.2. **CVE ID: CVE-2016-4846**	http://www.securebrain.co.jp/about/news/2016/08/160817.html	A-SEC-PHISH-010517/114

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

Shopware					
Shopware NA					
Execute Code	21-04-2017	10	The backend/Login/load/ script in Shopware before 5.1.5 allows remote attackers to execute arbitrary code. **CVE ID: CVE-2016-3109**	https://github.com/shopware/shopware/commit/d73e9031a5b2ab6e918eb86d1e2b2e873cd3558d	A-SHO-SHOPW-010517/115
Squirrelmail					
Squirrelmail NA					
Execute Code	20-04-2017	9	SquirrelMail 1.4.22 (and other versions before 20170427_0200-SVN) allows post-authentication remote code execution via a sendmail.cf file that is mishandled in a popen call. It's possible to exploit this vulnerability to execute arbitrary shell commands on the remote server. The problem is in the Deliver_SendMail.class.php with the initStream function that uses escapeshellcmd() to sanitize the sendmail command before executing it. The use of escapeshellcmd() is not correct in this case since it doesn't escape whitespaces, allowing the injection of arbitrary command parameters. The problem is in -f$envelopefrom within the sendmail command line. Hence, if the target server uses sendmail and SquirrelMail is configured to use it as a command-line program, it's possible to trick sendmail into using an attacker-provided configuration file that triggers the execution of an arbitrary command. For exploitation, the attacker must	NA	A-SQU-SQUIR-010517/116

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

			upload a sendmail.cf file as an email attachment, and inject the sendmail.cf filename with the -C option within the "Options > Personal Informations > Email Address" setting. **CVE ID: CVE-2017-7692**		
Tenable					
Appliance; Nessus Tenable Network Security develops unified security monitoring solutions for securing enterprise networks.					
NA	21-04-2017	10	Tenable Appliance 3.5 - 4.4.0, and possibly prior versions, contains a flaw in the simpleupload.py script in the Web UI. Through the manipulation of the tns_appliance_session_user parameter, a remote attacker can inject arbitrary commands. **CVE ID: CVE-2017-8051**	http://www.tenable.com/security/tns-2017-07	A-TEN-APPLI-010517/117
NA	21-04-2017	5	Tenable Appliance 4.4.0, and possibly prior, contains a flaw in the Web UI that allows for the unauthorized manipulation of the admin password. **CVE ID: CVE-2017-8050**	http://www.tenable.com/security/tns-2017-07	A-TEN-APPLI-010517/118
NA	19-04-2017	7.2	Nessus 6.10.x before 6.10.5 was found to be vulnerable to a local privilege escalation issue due to insecure permissions when running in Agent Mode. **CVE ID: CVE-2017-7850**	https://www.tenable.com/security/tns-2017-10	A-TEN-NESSU-010517/119
Unitrends					
Enterprise Backup NA					
Execute Code	19-04-2017	9	An authenticated user of Unitrends Enterprise Backup before 9.1.2 can execute arbitrary OS commands by sending a specially crafted filename to the /api/restore/download-files endpoint, related to the downloadFiles function in api/includes/restore.php. **CVE ID: CVE-2017-7283**	NA	A-UNI-ENTER-010517/120

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

Gain Information; File Inclusion	19-04-2017	7.1	An issue was discovered in Unitrends Enterprise Backup before 9.1.1. The function downloadFile in api/includes/restore.php blindly accepts any filename passed to /api/restore/download as valid. This allows an authenticated attacker to read any file in the filesystem that the web server has access to, aka Local File Inclusion (LFI). **CVE ID: CVE-2017-7282**	NA	A-UNI-ENTER-010517/121
Unrtf Project					
Unrtf NA					
Overflow	21-04-2017	5	Multiple stack-based buffer overflows in unrtf 0.21.9 allow remote attackers to cause a denial-of-service by writing a negative integer to the (1) cmd_expand function, (2) cmd_emboss function, or (3) cmd_engrave function. **CVE ID: CVE-2016-10091**	http://hg.savannah.gnu.org/hgweb/unrtf/rev/3b16893a6406	A-UNR-UNRTF-010517/122
Weechat					
Weechat NA					
Overflow	23-04-2017	5	WeeChat before 1.7.1 allows a remote crash by sending a filename via DCC to the IRC plugin. This occurs in the irc_ctcp_dcc_filename_without_quotes function during quote removal, with a buffer overflow. **CVE ID: CVE-2017-8073**	https://weechat.org/download/security/	A-WEE-WEECH-010517/123
Wondercms					
Wondercms NA					
CSRF	20-04-2017	6.8	WonderCMS before 2.0.3 has CSRF because of lack of a token in an unspecified context. **CVE ID: CVE-2017-7951**	https://www.wondercms.com/forum/viewtopic.php?f=8&p=1684	A-WON-WONDE-010517/124
Yeager					

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

Yeager Cms yeager is a new web CMS aiming to become the most cost/time-effective platform for medium and large sites and applications.					
NA	24-04-2017	6.4	Multiple server-side request forgery (SSRF) vulnerabilities in Yeager CMS 1.2.1 allow remote attackers to trigger outbound requests and enumerate open ports via the dbhost parameter to libs/org/adodb_lite/tests/test_adodb_lite.php, libs/org/adodb_lite/tests/test_datadictionary.php, or libs/org/adodb_lite/tests/test_adodb_lite_sessions.php. **CVE ID: CVE-2015-7570**	NA	A-YEA-YEAGE-010517/125
Execute Code; Sql	24-04-2017	7.5	SQL injection vulnerability in "yeager/y.php/tab_USERLIST" in Yeager CMS 1.2.1 allows local users to execute arbitrary SQL commands via the "pagedir_orderby" parameter. **CVE ID: CVE-2015-7569**	NA	A-YEA-YEAGE-010517/126
Sql	24-04-2017	7.5	SQL injection vulnerability in the password recovery feature in Yeager CMS 1.2.1 allows remote attackers to change the account credentials of known users via the "userEmail" parameter. **CVE ID: CVE-2015-7568**	NA	A-YEA-YEAGE-010517/127
Zohocorp					
Password Manager Pro NA					
CSRF	20-04-2017	6	Cross-site request forgery (CSRF) vulnerability in ManageEngine Password Manager Pro before 8.5 (Build 8500). **CVE ID: CVE-2016-1161**	NA	A-ZOH-PASSW-010517/128
Application; Operating System (A/OS)					
Clusterlabs/Fedoraproject;Redhat					
PCS/Fedora/Enterprise Linux Linux is a Unix-like computer operating system assembled under the model of free and open-source software development and distribution.					
CSRF	21-04-2017	6.8	Cross-site request forgery (CSRF)	https://bug	A-CLU-

			vulnerability in pcsd web UI in pcs before 0.9.149. **CVE ID: CVE-2016-0720**	zilla.redhat.com/show_bug.cgi?id=1299614	PCS/F-010517/129
Debian/Digium					
Debian Linux/Asterisk;Certified Asterisk Linux is a Unix-like computer operating system assembled under the model of free and open-source software development and distribution.					
DoS	17-04-2017	5	chain_sip in Asterisk Open Source 11.x before 11.23.1 and 13.x 13.11.1 and Certified Asterisk 11.6 before 11.6-cert15 and 13.8 before 13.8-cert3 allows remote attackers to cause a denial of service (port exhaustion). **CVE ID: CVE-2016-7551**	https://bugzilla.redhat.com/show_bug.cgi?id=1374733	A-DEB-DEBIA-010517/130
Debian;Novell;Opensuse Project/Lhasa Project					
Debian Linux/Leap/Opensuse/Lhasa Linux is a Unix-like computer operating system assembled under the model of free and open-source software development and distribution.					
Execute Code	21-04-2017	6.8	Integer underflow in the decode_level3_header function in lib/lha_file_header.c in Lhasa before 0.3.1 allows remote attackers to execute arbitrary code via a crafted archive. **CVE ID: CVE-2016-2347**	https://github.com/fragglet/lhasa/releases/tag/v0.3.1	A-DEB-DEBIA-010517/131
Fedoraproject/Spring-amqp Project					
Fedora/Spring-amqp NA					
Execute Code	21-04-2017	7.5	org.springframework.core.serializer.DefaultDeserializer in Spring AMQP before 1.5.5 allows remote attackers to execute arbitrary code. **CVE ID: CVE-2016-2173**	https://pivotal.io/security/ CVE-2016-2173	A-FED-FEDOR-010517/132
Operating System (OS)					
Apple					
Apple Tv;Iphone Os;Mac Os X Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch, iOS, macOS, watchOS and more.					
DoS Execute Code Overflow Memory	20-04-2017	9.3	Heap-based buffer overflow in IOHIDFamily in Apple iOS before 9.3.2, OS X before 10.11.5, and tvOS before 9.2.1 allows attackers to	https://support.apple.com/en-in/HT2065	O-APP-APPLE-010517/133

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

Corruption			execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app. **CVE ID: CVE-2016-4650**	64	
Cisco					
Ios Xe Cisco Networking Software (IOS, XE, XR, and NX-OS) is the world's most widely deployed networking software.					
DoS	20-04-2017	6.3	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem of Cisco IOS XE 3.16 could allow an authenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to a race condition that could occur when the affected software processes an SNMP read request that contains certain criteria for a specific object ID (OID) and an active crypto session is disconnected on an affected device. An attacker who can authenticate to an affected device could trigger this vulnerability by issuing an SNMP request for a specific OID on the device. A successful exploit will cause the device to restart due to an attempt to access an invalid memory region. The attacker does not control how or when crypto sessions are disconnected on the device. Cisco Bug IDs: CSCvb94392. **CVE ID: CVE-2017-6615**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-ios-xe-snmp	O-CIS-IOS X-010517/134
IOS;Ios Xe Cisco Networking Software (IOS, XE, XR, and NX-OS) is the world's most widely deployed networking software.					
DoS; Overflow	20-04-2017	7.8	Multiple vulnerabilities in the EnergyWise module of Cisco IOS (12.2 and 15.0 through 15.6) and Cisco IOS XE (3.2 through 3.18) could allow an unauthenticated, remote attacker to cause a buffer	https://tools.cisco.com/security/center/content/CiscoSecurityAdviso	O-CIS-IOSI-010517/135

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

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

			overflow condition or a reload of an affected device, leading to a denial of service (DoS) condition. These vulnerabilities are due to improper parsing of crafted EnergyWise packets destined to an affected device. An attacker could exploit these vulnerabilities by sending crafted EnergyWise packets to be processed by an affected device. An exploit could allow the attacker to cause a buffer overflow condition or a reload of the affected device, leading to a DoS condition. Cisco IOS Software and Cisco IOS XE Software support EnergyWise for IPv4 communication. Only IPv4 packets destined to a device configured as an EnergyWise domain member can trigger these vulnerabilities. IPv6 packets cannot be used to trigger these vulnerabilities. Cisco Bug ID CSCut50727. **CVE ID: CVE-2017-3863**	ry/cisco-sa-20170419-energywise	
DoS; Overflow	20-04-2017	7.8	Multiple vulnerabilities in the EnergyWise module of Cisco IOS (12.2 and 15.0 through 15.6) and Cisco IOS XE (3.2 through 3.18) could allow an unauthenticated, remote attacker to cause a buffer overflow condition or a reload of an affected device, leading to a denial of service (DoS) condition. These vulnerabilities are due to improper parsing of crafted EnergyWise packets destined to an affected device. An attacker could exploit these vulnerabilities by sending crafted EnergyWise packets to be processed by an affected device. An exploit could allow the attacker to cause a buffer overflow condition or a reload of the affected device, leading to a DoS condition. Cisco IOS Software and Cisco IOS XE Software	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-energywise	O-CIS-IOS;I-010517/136

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 EnergyWise for IPv4 communication. Only IPv4 packets destined to a device configured as an EnergyWise domain member can trigger these vulnerabilities. IPv6 packets cannot be used to trigger these vulnerabilities. Cisco Bug ID CSCuu76493. **CVE ID: CVE-2017-3862**		
DoS Overflow	20-04-2017	7.8	Multiple vulnerabilities in the EnergyWise module of Cisco IOS (12.2 and 15.0 through 15.6) and Cisco IOS XE (3.2 through 3.18) could allow an unauthenticated, remote attacker to cause a buffer overflow condition or a reload of an affected device, leading to a denial of service (DoS) condition. These vulnerabilities are due to improper parsing of crafted EnergyWise packets destined to an affected device. An attacker could exploit these vulnerabilities by sending crafted EnergyWise packets to be processed by an affected device. An exploit could allow the attacker to cause a buffer overflow condition or a reload of the affected device, leading to a DoS condition. Cisco IOS Software and Cisco IOS XE Software support EnergyWise for IPv4 communication. Only IPv4 packets destined to a device configured as an EnergyWise domain member can trigger these vulnerabilities. IPv6 packets cannot be used to trigger these vulnerabilities. Cisco Bug ID CSCut47751. **CVE ID: CVE-2017-3861**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170419-energywise	O-CIS-IOS;I-010517/137
DoS Overflow	20-04-2017	7.8	Multiple vulnerabilities in the EnergyWise module of Cisco IOS (12.2 and 15.0 through 15.6) and Cisco IOS XE (3.2 through 3.18) could allow an unauthenticated, remote attacker to cause a buffer	https://tools.cisco.com/security/center/content/CiscoSecurityAdviso	O-CIS-IOS;I-010517/138

			overflow condition or a reload of an affected device, leading to a denial of service (DoS) condition. These vulnerabilities are due to improper parsing of crafted EnergyWise packets destined to an affected device. An attacker could exploit these vulnerabilities by sending crafted EnergyWise packets to be processed by an affected device. An exploit could allow the attacker to cause a buffer overflow condition or a reload of the affected device, leading to a DoS condition. Cisco IOS Software and Cisco IOS XE Software support EnergyWise for IPv4 communication. Only IPv4 packets destined to a device configured as an EnergyWise domain member can trigger these vulnerabilities. IPv6 packets cannot be used to trigger these vulnerabilities. Cisco Bug ID CSCur29331. **CVE ID: CVE-2017-3860**	ry/cisco-sa-20170419-energywise	
D-link					
Dap-2230 Firmware; Dap-2310 Firmware; Dap-2330 Firmware ; Dap-2360 Firmware; Dap-2553 Firmware; Dap-2660 Firmware; Dap-2690 Firmware; Dap-2695 Firmware; Dap-3320 Firmware; Dap-3662 Firmware NA					
Overflow	21-04-2017	10	Buffer overflow in D-Link DAP-2310 2.06 and earlier, DAP-2330 1.06 and earlier, DAP-2360 2.06 and earlier, DAP-2553 H/W ver. B1 3.05 and earlier, DAP-2660 1.11 and earlier, DAP-2690 3.15 and earlier, DAP-2695 1.16 and earlier, DAP-3320 1.00 and earlier, and DAP-3662 1.01 and earlier allows remote attackers to have unspecified impact via a crafted 'dlink_uid' cookie. **CVE ID: CVE-2016-1558**	http://www.dlink.com/mk/mk/support/support-news/2016/march/16/firmadyne-cve_2016_1558-cve_2016_1559	O-D-L-DAP-2-010517/139
Dvg-n5402sp Firmware NA					

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	24-04-2017	5	Directory traversal vulnerability in D-Link DVG-N5402SP with firmware W1000CN-00, W1000CN-03, or W2000EN-00 allows remote attackers to read sensitive information via a .. (dot dot) in the errorpage parameter. **CVE ID: CVE-2015-7245**		O-D-L-DVG-N-010517/140
Dvg-n5402sp Firmware NA					
Gain Information	24-04-2017	7.8	D-Link DVG-N5402SP with firmware W1000CN-00, W1000CN-03, or W2000EN-00 discloses usernames, passwords, keys, values, and web account hashes (super and admin) in plaintext when running a configuration backup, which allows remote attackers to obtain sensitive information. **CVE ID: CVE-2015-7247**	NA	O-D-L-DVG-N-010517/141
NA	24-04-2017	10	D-Link DVG-N5402SP with firmware W1000CN-00, W1000CN-03, or W2000EN-00 has a default password of root for the root account and tw for the tw account, which makes it easier for remote attackers to obtain administrative access. **CVE ID: CVE-2015-7246**	NA	O-D-L-DVG-N-010517/142
Exagrid					
Ex10000e Firmware;Ex13000e Firmware;Ex21000e Firmware;Ex3000 Firmware;Ex32000e Firmware;Ex40000e Firmware;Ex5000 Firmware;Ex7000 Firmware NA					
NA	21-04-2017	10	ExaGrid appliances with firmware before 4.8 P26 have a default password of (1) inflection for the root shell account and (2) support for the support account in the web interface, which allows remote attackers to obtain administrative access via an SSH or HTTP session. **CVE ID: CVE-2016-1560**	NA	O-EXA-EX100-010517/143
Gain Information	21-04-2017	5	ExaGrid appliances with firmware before 4.8 P26 have a default SSH	NA	O-EXA-EX100-

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

			public key in the authorized_keys file for root, which allows remote attackers to obtain SSH access by leveraging knowledge of a private key from another installation or a firmware image. **CVE ID: CVE-2016-1561**		010517/144
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.					
DoS	21-04-2017	7.8	Android allows users to cause a denial of service. **CVE ID: CVE-2016-0833**	NA	O-GOO-ANDRO-010517/145
Execute Code	17-04-2017	10	The Qualcomm GPS subsystem in Android on Android One devices allows remote attackers to execute arbitrary code. **CVE ID: CVE-2016-6727**	https://source.android.com/security/bulletin/2016-11-01	O-GOO-ANDRO-010517/146
	17-04-2017	10	Unspecified vulnerability in Qualcomm components in Android on Nexus 6 and Android One devices. **CVE ID: CVE-2016-6726**	https://source.android.com/security/bulletin/2016-11-01	O-GOO-ANDRO-010517/147
Linux					
Linux Kernel The Linux kernel is a monolithic Unix-like computer operating system kernel.					
DoS; Overflow; Memory Corruption	23-04-2017	7.2	crypto/ccm.c in the Linux kernel 4.9.x and 4.10.x through 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8065**	https://github.com/torvalds/linux/commit/3b30460c5b0ed762be75a004e924ec3f8711e032	O-LIN-LINUX-010517/148
DoS; Overflow; Memory Corruption	23-04-2017	7.2	drivers/char/virtio_console.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or	https://github.com/torvalds/linux/commit/c4baad50297d84bde1a	O-LIN-LINUX-010517/149

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

			memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8067**	7ad45e50c73adae4a2192	
DoS; Overflow	23-04-2017	7.2	drivers/media/usb/dvb-usb/cxusb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8063**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.10.12	O-LIN-LINUX-010517/150
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/media/usb/dvb-usb/dvb-usb-firmware.c in the Linux kernel 4.9.x and 4.10.x before 4.10.7 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8061**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.10.7	O-LIN-LINUX-010517/151
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/media/usb/dvb-usb/dw2102.c in the Linux kernel 4.9.x and 4.10.x before 4.10.4 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8062**	http://www.kernel.org/pub/linux/kernel/v4.x/ChangeLog-4.10.4	O-LIN-LINUX-010517/152
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/media/usb/dvb-usb-v2/dvb_usb_core.c in the Linux kernel 4.9.x and 4.10.x before 4.10.12 interacts incorrectly with	http://www.kernel.org/pub/linux/kernel/v	O-LIN-LINUX-010517/153

			the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8064**	4.x/Change Log-4.10.12	
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/net/can/usb/gs_usb.c in the Linux kernel 4.9.x and 4.10.x before 4.10.2 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8066**	https://github.com/torvalds/linux/commit/c919a3069c775c1c876bec55e00b2305d5125caa	O-LIN-LINUX-010517/154
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/net/usb/catc.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8070**	https://github.com/torvalds/linux/commit/2d6a0e9de03ee658a9adc3bfb2f0ca55dff1e478	O-LIN-LINUX-010517/155
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/net/usb/pegasus.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8068**	https://github.com/torvalds/linux/commit/5593523f968bc86d42a035c6df47d5e0979b5ace	O-LIN-LINUX-010517/156
DoS Overflow Memory Corruption	23-04-2017	7.2	drivers/net/usb/rtl8150.c in the Linux kernel 4.9.x before 4.9.11 interacts incorrectly with the CONFIG_VMAP_STACK option,	https://github.com/torvalds/linux/commit/7	O-LIN-LINUX-010517/157

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

			which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist. **CVE ID: CVE-2017-8069**	926aff5c57b577ab0f43364ff0c59d968f6a414	
DoS	19-04-2017	7.2	The cookie feature in the packet action API implementation in net/sched/act_api.c in the Linux kernel 4.11.x through 4.11-rc7 mishandles the tb nlattr array, which allows local users to cause a denial of service (uninitialized memory access and refcount underflow, and system hang or crash) or possibly have unspecified other impact via "tc filter add" commands in certain contexts. NOTE: this does not affect stable kernels, such as 4.10.x, from kernel.org. **CVE ID: CVE-2017-7979**		O-LIN-LINUX-010517/158
NA	23-04-2017	7.2	The cp2112_gpio_direction_input function in drivers/hid/hid-cp2112.c in the Linux kernel 4.9.x before 4.9.9 does not have the expected EIO error status for a zero-length report, which allows local users to have an unspecified impact via unknown vectors. **CVE ID: CVE-2017-8072**	https://github.com/torvalds/linux/commit/8e9faa15469ed7c7467423db4c62aeed3ff4cae3	O-LIN-LINUX-010517/159
Bypass	16-04-2017	7.2	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.		O-LIN-LINUX-010517/160

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-2017-7889		
DoS	18-04-2017	7.8	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c. **CVE ID: CVE-2017-7645**	https://github.com/torvalds/linux/commit/e6838a29ecb484c97e4efef9429643b9851fba6e	O-LIN-LINUX-010517/161
Moxa					
Awk-3131a Firmware NA					
	20-04-2017	9	An exploitable OS Command Injection vulnerability exists in the web application 'ping' functionality of Moxa AWK-3131A Wireless Access Points running firmware 1.1. Specially crafted web form input can cause an OS Command Injection resulting in complete compromise of the vulnerable device. An attacker can exploit this vulnerability remotely. **CVE ID: CVE-2016-8721**	http://www.talosintelligence.com/reports/TALOS-2016-0235/	O-MOX-AWK-3-010517/162
Netgear					
Wn604 Firmware;Wn802tv2 Firmware;Wnap320 Firmware;Wndap210v2 Firmware;Wndap350 Firmware;Wndap360 Firmware;Wndap660 Firmware; Wn604 Firmware;Wnap320 Firmware;Wnd930 Firmware;Wndap210v2 Firmware; Wnap320 Firmware NA					
Execute Code	21-04-2017	10	(1) boardData102.php, (2) boardData103.php, (3) boardDataJP.php, (4) boardDataNA.php, and (5) boardDataWW.php in Netgear WN604 before 3.3.3 and WN802Tv2, WNAP210v2, WNAP320, WNDAP350, WNDAP360, and WNDAP660 before 3.5.5.0 allow remote attackers to execute arbitrary commands. **CVE ID: CVE-2016-1555**	https://kb.netgear.com/30480/CVE-2016-1555-Notification?cid=wmt_netgear_organic	O-NET-WN604-010517/163
Gain Information	21-04-2017	5	Information disclosure in Netgear WN604 before 3.3.3; WNAP210,	https://kb.netgear.co	O-NET-WN604-

			WNAP320, WNDAP350, and WNDAP360 before 3.5.5.0; and WND930 before 2.0.11 allows remote attackers to read the wireless WPS PIN or passphrase by visiting unauthenticated webpages. **CVE ID: CVE-2016-1556**	m/30481/CVE-2016-1556-Notification?cid=wmt_netgear_organic	010517/164
Gain Information	21-04-2017	5	Netgear WNAP320, WNDAP350, and WNDAP360 before 3.5.5.0 reveal wireless passwords and administrative usernames and passwords over SNMP. **CVE ID: CVE-2016-1557**	https://kb.netgear.com/30482/CVE-2016-1557-Notification?cid=wmt_netgear_organic	O-NET-WNAP3-010517/165
Samsung					
Samsung Mobile NA					
Gain Information	19-04-2017	5	Samsung Android devices with L(5.0/5.1), M(6.0), and N(7.x) software allow attackers to obtain sensitive information by reading a world-readable log file after an unexpected reboot. The Samsung ID is SVE-2017-8290. **CVE ID: CVE-2017-7978**	http://security.samsungmobile.com/smrupdate.html#SMR-APR-2017	O-SAM-SAMSU-010517/166
Tp-link					
Tl-sg108e Firmware NA					
NA	23-04-2017	5	On the TP-Link TL-SG108E 1.0, a remote attacker could retrieve credentials from "SEND data" log lines where passwords are encoded in hexadecimal. This affects the 1.1.2 Build 20141017 Rel.50749 firmware. **CVE ID: CVE-2017-8074**	NA	O-TP--TL-SG-010517/167
NA	23-04-2017	5	On the TP-Link TL-SG108E 1.0, a remote attacker could retrieve credentials from "Switch Info" log lines where passwords are in cleartext. This affects the 1.1.2 Build 20141017 Rel.50749 firmware.	NA	O-TP--TL-SG-010517/168

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-2017-8075		
NA	23-04-2017	7.8	On the TP-Link TL-SG108E 1.0, admin network communications are RC4 encoded, even though RC4 is deprecated. This affects the 1.1.2 Build 20141017 Rel.50749 firmware. **CVE ID: CVE-2017-8076**	https://chmod750.com/2017/04/23/vulnerability-disclosure-tp-link/	O-TP--TL-SG-010517/169
NA	23-04-2017	5	On the TP-Link TL-SG108E 1.0, the upgrade process can be requested remotely without authentication (httpupg.cgi with a parameter called cmd). This affects the 1.1.2 Build 20141017 Rel.50749 firmware. **CVE ID: CVE-2017-8078**	NA	O-TP--TL-SG-010517/170
NA	23-04-2017	5	On the TP-Link TL-SG108E 1.0, there is a hard-coded ciphering key (a long string beginning with Ei2HNryt). This affects the 1.1.2 Build 20141017 Rel.50749 firmware. **CVE ID: CVE-2017-8077**	https://chmod750.com/2017/04/23/vulnerability-disclosure-tp-link/	O-TP--TL-SG-010517/171
Watchguard					
Fireware NA					
NA	22-04-2017	5	WatchGuard Fireware allows user enumeration, e.g., in the Firebox XML-RPC login handler. A login request that contains a blank password sent to the XML-RPC agent in Fireware v11.12.1 and earlier returns different responses for valid and invalid usernames. An attacker could exploit this vulnerability to enumerate valid usernames on an affected Firebox. **CVE ID: CVE-2017-8055**	NA	O-WAT-FIREW-010517/172
DoS	22-04-2017	5	WatchGuard Fireware v11.12.1 and earlier mishandles requests referring to an XML External Entity (XXE), in the XML-RPC agent. This causes the Firebox wgagent process to crash. This process crash ends all authenticated sessions to the	NA	O-WAT-FIREW-010517/173

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

			Firebox, including management connections, and prevents new authenticated sessions until the process has recovered. The Firebox may also experience an overall degradation in performance while the wgagent process recovers. An attacker could continuously send XML-RPC requests that contain references to external entities to perform a limited Denial of Service (DoS) attack against an affected Firebox. **CVE ID: CVE-2017-8056**		
Zyxel					
Wre6505 Firmware NA					
NA	19-04-2017	10	Zyxel WRE6505 devices have a default TELNET password of 1234 for the root and admin accounts, which makes it easier for remote attackers to conduct DNS hijacking attacks by reconfiguring the built-in dnshijacker process. **CVE ID: CVE-2017-7964**	https://www.oxy-gen.mobi/blog.html	O-ZYX-WRE65-010517/174

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