



National Critical Information Infrastructure Protection Centre

CVE Report

01-15 Oct 2017

Vol. 04 No.17

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application (A)					
Akka					
Http Server					
DoS Overflow	04-10-2017	5	Akka HTTP versions <= 10.0.5 Illegal Media Range in Accept Header Causes StackOverflowError Leading to Denial of Service CVE ID:CVE-2017-1000118	https://doc.akka.io/docs/akka-http/10.0.6/security/2017-05-03-illegal-media-range-in-accept-header-causes-stackoverflowerror.html	A-AKK-HTTP-161017/1
Apache					
Wicket					
Gain Information	02-10-2017	5	In Apache Wicket 1.5.10 or 6.13.0, by issuing requests to special urls handled by Wicket, it is possible to check for the existence of particular classes in the classpath and thus check whether a third party library with a known security vulnerability is in use. CVE ID:CVE-2014-0043	https://lists.apache.org/thread.html/d95e962f2f059a09f5abf7086c3f4ed22d2ae2c21499d0de95d4435d@1392986987@%3Cannounce.wicket.apache.org%3E	A-APA-WICKE-161017/2
Geode					
DoS Gain Information	02-10-2017	5.8	When an Apache Geode cluster before v1.2.1 is operating in secure mode, an unauthenticated client can enter multi-user authentication mode and send metadata messages. These metadata operations could leak information about application data types. In addition, an attacker could perform a denial of service attack on the cluster. CVE ID:CVE-2017-9797	http://mail-archives.apache.org/mod_mbox/geode-user/201709.mbox/%3cCAEwgeHrbb7JS8Nygrh7geyFvW4bMZ3AdCmPOzMfvbniipz0bA@mail.gmail.com%3e	A-APA-GEODE-161017/3
Atlassian					

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bamboo					
Execute Code	02-10-2017	6.5	Bamboo 2.2 before 5.8.5 and 5.9.x before 5.9.7 allows remote attackers with access to the Bamboo web interface to execute arbitrary Java code via an unspecified resource. CVE ID:CVE-2015-6576	https://confluence.atlassian.com/x/Hw7RLg	A-ATL-BAMBO-161017/4
Ciphershed;Truecrypt;Veracrypt					
Ciphershed/Truecrypt/Veracrypt					
Gain Privileges	02-10-2017	7.2	The IsDriveLetterAvailable method in Driver/Ntdriver.c in TrueCrypt 7.0, VeraCrypt before 1.15, and CipherShed, when running on Windows, does not properly validate drive letter symbolic links, which allows local users to mount an encrypted volume over an existing drive letter and gain privileges via an entry in the /GLOBAL?? directory. CVE ID:CVE-2015-7358	https://veracrypt.codeplex.com/wikipage?title=Release%20Notes	A-CIP-CIPHE-161017/8
Cisco					
Spark					
Execute Code XSS	05-10-2017	3.5	A vulnerability in the web UI of Cisco Spark Messaging Software could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. The vulnerability is due to insufficient input validation by the web UI of the affected software. An attacker could exploit this vulnerability by injecting XSS content into the web UI of the affected software. A successful exploit could allow the attacker to force a user to execute code of the attacker's choosing or allow the attacker to retrieve sensitive information from the user. Cisco Bug IDs: CSCvf70587, CSCvf70592.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-sprk	A-CIS-SPARK-161017/9

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			CVE ID:CVE-2017-12269		
Adaptive Security Appliance					
Execute Code XSS	05-10-2017	4.3	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device, aka HREF XSS. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information. The vulnerability exists in the Cisco Adaptive Security Appliance (ASA) Software when the WEBVPN feature is enabled. Cisco Bug IDs: CSCve91068. CVE ID:CVE-2017-12265	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-asa1	A-CIS-ADAPT-161017/10
Unified Communications Manager					
XSS	05-10-2017	4.3	A vulnerability in the web-based UI of Cisco Unified Communications Manager could allow an unauthenticated, remote attacker to execute a cross-frame scripting (XFS) attack. The vulnerability exists because the affected software does not provide sufficient protections for HTML inline frames (iframes). An attacker could exploit this vulnerability by	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-ucm	A-CIS-UNIFI-161017/11

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			directing a user of the affected software to an attacker-controlled web page that contains a malicious HTML inline frame. A successful exploit could allow the attacker to conduct click-jacking or other types of client-side browser attacks. Cisco Bug IDs: CSCve60993. CVE ID:CVE-2017-12258		

Webex Meetings Server

Execute Code XSS	05-10-2017	4.3	A vulnerability in the web framework of Cisco WebEx Meetings Server could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of an affected system. The vulnerability is due to insufficient input validation of some parameters that are passed to the web server of the affected system. An attacker could exploit this vulnerability by convincing a user to follow a malicious link or by intercepting a user request and injecting malicious code into the request. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected web interface or allow the attacker to access sensitive browser-based information. Cisco Bug IDs: CSCve96608. CVE ID:CVE-2017-12257	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-wms	A-CIS-WEBEX-161017/12
------------------	------------	-----	---	---	-----------------------

Wide Area Application Services

NA	05-10-2017	7.1	A vulnerability in the Akamai Connect feature of Cisco Wide Area Application Services (WAAS) Appliances could allow an unauthenticated, remote attacker to cause a denial-of-service (DoS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-waas	A-CIS-WIDE - 161017/13
----	------------	-----	--	---	------------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			condition on an affected device. The vulnerability is due to certain file-handling inefficiencies of the affected system. An attacker could exploit this vulnerability by directing client systems to access a corrupted file that the client systems cannot decompress correctly. A successful exploit could allow the attacker to cause the affected device to crash or hang unexpectedly and result in a DoS condition that may require manual intervention to regain normal operating conditions. Cisco Bug IDs: CSCve82472. CVE ID: CVE-2017-12256		

Dasinfomedia

Human Resource Management System

Sql	02-10-2017	6.5	WPHRM Human Resource Management System for WordPress 1.0 allows SQL Injection via the employee_id parameter. CVE ID: CVE-2017-14848	NA	A-DAS-HUMAN-161017/16
-----	------------	-----	--	----	-----------------------

Docker

Docker

NA	06-10-2017	4.6	Docker before 1.5 allows local users to have unspecified impact via vectors involving unsafe /tmp usage. CVE ID: CVE-2014-0047	https://bugzilla.redhat.com/show_bug.cgi?id=1063549	A-DOC-DOCKE-161017/17
----	------------	-----	---	---	-----------------------

EMC

Appsync

DoS	02-10-2017	5	EMC AppSync host plug-in versions 3.5 and below (Windows platform only) includes a denial of service (DoS) vulnerability that could potentially be exploited by malicious users to compromise the affected system. CVE ID: CVE-2017-8018	http://seclists.org/fulldisclosure/2017/Sep/75	A-EMC-APPSY-161017/18
-----	------------	---	---	---	-----------------------

Emtec

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):

CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pyrobatchftp					
DoS Overflow	05-10-2017	5	EmTec PyroBatchFTP before 3.18 allows remote servers to cause a denial of service (application crash). CVE ID: CVE-2017-15035	https://www.emtec.com/downloads/pyrobatchftp/pyrobatchftp318_changes.txt	A-EMT-PYROB-161017/19
Formget					
Easy Contact Form Solution					
XSS	06-10-2017	4.3	Cross-site scripting (XSS) vulnerability in the Easy Contact Form Solution plugin before 1.7 for WordPress allows remote attackers to inject arbitrary web script or HTML via the value parameter in a master_response action to wp-admin/admin-ajax.php. CVE ID: CVE-2014-7240	NA	A-FOR-EASY-161017/23
Frappe					
Frappe					
Execute Code Sql	04-10-2017	6.5	[ERPNext][Frappe Version <= 7.1.27] SQL injection vulnerability in frappe.share.get_users allows remote authenticated users to execute arbitrary SQL commands via the fields parameter. CVE ID: CVE-2017-1000120	http://tech.mantz-it.com/2016/12/sql-injection-in-frappe-framework.html	A-FRA-FRAPP-161017/24
Freedesktop					
Poppler					
DoS	01-10-2017	5	The FoFiTrueType::getCFFBlock function in FoFiTrueType.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability due to lack of validation of a table pointer, which allows an attacker to launch a denial of service attack. CVE ID: CVE-2017-14977	https://bugs.freedesktop.org/show_bug.cgi?id=103045	A-FRE-POPPL-161017/25
DoS Overflow	01-10-2017	5	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a heap-based buffer over-read vulnerability if an out-of-bounds font dictionary index is encountered, which allows an	https://cgit.freedesktop.org/poppler/poppler/commit/?id=da63c35549e8852a410946ab016a3f25	A-FRE-POPPL-161017/26

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			attacker to launch a denial of service attack. CVE ID: CVE-2017-14976	ac701bdf	
DoS	01-10-2017	5	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability because a data structure is not initialized, which allows an attacker to launch a denial of service attack. CVE ID: CVE-2017-14975	https://bugzilla.reedesktop.org/show_bug.cgi?id=102653	A-FRE-POPPL-161017/27

GE

Intelligent Platforms Proficy Hmi/scada Cimplicity

Execute Code Overflow	05-10-2017	4.9	A Stack-based Buffer Overflow issue was discovered in GE CIMPLICITY Versions 9.0 and prior. A function reads a packet to indicate the next packet length. The next packet length is not verified, allowing a buffer overwrite that could lead to an arbitrary remote code execution. CVE ID: CVE-2017-12732	NA	A-GE-INTEL-161017/28
-----------------------	------------	-----	---	----	----------------------

GNU

Binutils

DoS	04-10-2017	4.3	decode_line_info in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted ELF file. CVE ID: CVE-2017-15025	NA	A-GNU-BINUT-161017/29
DoS	04-10-2017	4.3	find_abstract_instance_name in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (infinite recursion and application crash) via a crafted ELF file. CVE-2017-15024	NA	A-GNU-BINUT-161017/30

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
DoS	04-10-2017	4.3	read_formatted_entries in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not properly validate the format count, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to concat_filename. CVE ID: CVE-2017-15023	NA	A-GNU-BINUT-161017/31
DoS	04-10-2017	4.3	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, does not validate the DW_AT_name data type, which allows remote attackers to cause a denial of service (bfd_hash_hash NULL pointer dereference, or out-of-bounds access, and application crash) via a crafted ELF file, related to scan_unit_for_symbols and parse_comp_unit. CVE ID: CVE-2017-15022	NA	A-GNU-BINUT-161017/32
DoS Overflow	04-10-2017	4.3	bfd_get_debug_link_info_1 in opncls.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file, related to bfd_getl32. CVE ID: CVE-2017-15021	NA	A-GNU-BINUT-161017/33
DoS	01-10-2017	4.3	The *_get_synthetic_syntab functions in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandle the failure of a certain canonicalization step, which allows remote attackers to	https://sourceware.org/git/gitweb.cgi?p=binutils-gdb.git;h=e70c19e3a4c26e9c1ebf0c9170d105039	A-GNU-BINUT-161017/34

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			cause a denial of service (NULL pointer dereference and application crash) via a crafted ELF file, related to elf32-i386.c and elf64-x86-64.c. CVE ID: CVE-2017-14974	b56d7cf	
DoS Overflow	04-10-2017	6.8	dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, mishandles pointers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted ELF file, related to parse_die and parse_line_table, as demonstrated by a parse_die heap-based buffer over-read. CVE ID: CVE-2017-15020	NA	A-GNU-BINUT-161017/35

Golang

GO

NA	04-10-2017	5	The net/http package's Request.ParseMultipartForm method starts writing to temporary files once the request body size surpasses the given "maxMemory" limit. It was possible for an attacker to generate a multipart request crafted such that the server ran out of file descriptors. CVE ID: CVE-2017-100098	https://groups.google.com/forum/#%21msg/golang-dev/4NdLzS8sls8/ulz8QlnIBQAJ	A-GOL-GO-161017/36
NA	04-10-2017	5	On Darwin, user's trust preferences for root certificates were not honored. If the user had a root certificate loaded in their Keychain that was explicitly not trusted, a Go program would still verify a connection using that root certificate. CVE ID: CVE-2017-100097	https://github.com/golang/go/issues/18141	A-GOL-GO-161017/37

Google

Chrome

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
DoS Overflow	06-10-2017	4.3	Heap-based buffer overflow in Google Chrome before M40 allows remote attackers to cause a denial of service (unpaged memory write and process crash) via a crafted MP4 file. CVE ID: CVE-2015-1206	https://gist.github.com/bittorrent/3389/8fee7cdaa73d1d351ee9	A-GOO-CHROM-161017/38
Graphicsmagick					
Graphicsmagick					
DoS	03-10-2017	4.3	ReadDCMImage in coders/dcm.c in GraphicsMagick 1.3.26 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted DICOM image, related to the ability of DCM_ReadNonNativeImages to yield an image list with zero frames. CVE ID: CVE-2017-14994	https://sourceforge.net/p/graphicsmagick/bugs/512/	A-GRA-GRAPH-161017/39
DoS	03-10-2017	7.1	GraphicsMagick 1.3.26 allows remote attackers to cause a denial of service (excessive memory allocation) because of an integer underflow in ReadPCTImage in coders/pict.c. CVE ID: CVE-2017-14997	https://sourceforge.net/p/graphicsmagick/code/ci/0683f8724200495059606c03f04e0d589b33e8/	A-GRA-GRAPH-161017/40
HP					
Ucmdb Foundation Software					
XSS	05-10-2017	4.3	A remote cross-site scripting vulnerability in HP UCMDB Foundation Software versions 10.10, 10.11, 10.20, 10.21, 10.22, 10.30, 10.31, 10.32, and 10.33 could be remotely exploited to allow cross-site scripting. CVE ID: CVE-2017-14354	https://software.support.hpe.com/km/KM02977984	A-HP-UCMDB-161017/41
Execute Code	05-10-2017	6.8	A remote code execution vulnerability in HP UCMDB Foundation Software versions 10.10, 10.11, 10.20, 10.21, 10.22, 10.30, 10.31, 10.32, and 10.33, could be remotely exploited to allow code execution. CVE ID: CVE-	https://software.support.hpe.com/km/KM02977984	A-HP-UCMDB-161017/42

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			2017-14353		
IBM					
<i>Tivoli Storage Manager</i>					
NA	05-10-2017	2.1	IBM Spectrum Protect 7.1 and 8.1 (formerly Tivoli Storage Manager) disclosed unencrypted login credentials to VMware vCenter in the application trace output which could be obtained by a local user. IBM X-Force ID: 126875. CVE ID: CVE-2017-1378	http://www.ibm.com/support/docview.wss?uid=swg22006215	A-IBM-TIVOL-161017/43
DoS Gain Information	05-10-2017	2.1	IBM Spectrum Protect 7.1 and 8.1 (formerly Tivoli Storage Manager) Server uses weak encryption for the password. A database administrator may be able to decrypt the IBM Spectrum protect client or administrator password which can result in information disclosure or a denial of service. IBM X-Force ID: 126247. CVE ID: CVE-2017-1339	http://www.ibm.com/support/docview.wss?uid=swg22007936	A-IBM-TIVOL-161017/44
<i>Rational Engineering Lifecycle Manager</i>					
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 127587. CVE ID: CVE-2017-1429	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/45
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126862. CVE-2017-1369	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/46

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126857. CVE ID:CVE-2017-1364	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/47
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126686. CVE ID: CVE-2017-1359	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/48
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126243. CVE ID: CVE-2017-1335	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/49
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126242. CVE ID:CVE-2017-1334	http://www.ibm.com/support/docview.wss?uid=swg22008785	A-IBM-RATIO-161017/50
XSS	02-10-2017	3.5	IBM RELM 4.0, 5.0, and 6.0 is vulnerable to cross-site scripting.	http://www.ibm.com/support/do	A-IBM-RATIO-

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 125975. CVE ID: CVE-2017-1324	cview.wss?uid=SWG22008785	161017/51
WebSphere Commerce					
DoS	02-10-2017	5	IBM WebSphere Commerce 7.0 and 8.0 contains an unspecified vulnerability in Marketing ESpot's that could cause a denial of service. IBM X-Force ID: 131779. CVE ID: CVE-2017-1569	http://www.ibm.com/support/docview.wss?uid=SWG22008547	A-IBM-WEBSP-161017/52
Integration Bus; Websphere Message Broker					
Gain Information	03-10-2017	5	IBM WebSphere Message Broker (IBM Integration Bus 9.0 and 10.0) could allow an unauthorized user to obtain sensitive information about software versions that could lead to further attacks. IBM X-Force ID: 121341. CVE ID: CVE-2017-1126	http://www.ibm.com/support/docview.wss?uid=SWG22008470	A-IBM-INTEG-161017/53
Insights Foundation For Energy					
SS	02-10-2017	3.5	IBM Insights Foundation for Energy 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 126460. CVE ID: CVE-2017-1345	http://www.ibm.com/support/docview.wss?uid=SWG22009039	A-IBM-INSIG-161017/54
Sql	02-10-2017	6.5	IBM Insights Foundation for Energy 2.0 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or	http://www.ibm.com/support/docview.wss?uid=SWG22009039	A-IBM-INSIG-161017/55

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			delete information in the back-end database. IBM X-Force ID: 125719. CVE ID: CVE-2017-1311		
Imagemagick					
<i>Imagemagick</i>					
NA	02-10-2017	4.3	A use-after-free in RenderFreetype in MagickCore/annotate.c in ImageMagick 7.0.7-4 Q16 allows attackers to crash the application via a crafted font file, because the FT_Done_Glyph function (from FreeType 2) is called at an incorrect place in the ImageMagick code. CVE ID: CVE-2017-14989	https://github.com/ImageMagick/ImageMagick/issues/781	A-IMA-IMAGE-161017/56
NA	05-10-2017	5	ImageMagick version 7.0.7-2 contains a memory leak in ReadYUVImage in coders/yuv.c. CVE ID: CVE-2017-15033	https://github.com/ImageMagick/ImageMagick/commit/ef8f40689ac452398026c07da41656a7c87e4683	A-IMA-IMAGE-161017/57
NA	05-10-2017	7.5	ImageMagick version 7.0.7-2 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c. CVE ID: CVE-2017-15032	https://github.com/ImageMagick/ImageMagick/commit/241988ca28139ad970c1d9717c419f41e360ddb0	A-IMA-IMAGE-161017/58
NA	04-10-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadOneMNGImage in coders/png.c. CVE ID: CVE-2017-15017	https://github.com/ImageMagick/ImageMagick/issues/723	A-IMA-IMAGE-161017/59
NA	04-10-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadEnhMetaFile in coders/emf.c. CVE ID: CVE-2017-15016	https://github.com/ImageMagick/ImageMagick/issues/725	A-IMA-IMAGE-161017/60
NA	04-10-2017	7.5	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in	https://github.com/ImageMagick/ImageMagick/issues/725	A-IMA-IMAGE-161017/6

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID						
			PDFDelegateMessage coders/pdf.c. CVE ID: CVE-2017-15015	in sues/724	1						
Intelliants											
Subrion Cms											
CSRF	06-10-2017	6.8	There are CSRF vulnerabilities in Subrion CMS before 4.2.0 because of a logic error. Although there is functionality to detect CSRF, it is called too late in the ia.core.php code, allowing (for example) an attack against the query parameter to panel/database. CVE ID: CVE-2017-15063	https://github.com/intelliants/subrion/issues/547	A-INT-SUBRI-161017/62						
Ipswitch											
Imail Server											
Execute Code Overflow	02-10-2017	7.5	Stack based buffer overflow in Ipswitch IMail server up to and including 12.5.5 allows remote attackers to execute arbitrary code via unspecified vectors in IMmailSrv, aka ETRE or ETCTERARED. CVE ID: CVE-2017-12639	https://docs.ipswitch.com/_Messaging/IMailServer/v12.5.6/ReleaseNotes/index.htm#link8	A-IPS-IMAIL-161017/63						
Execute Code Overflow	02-10-2017	7.5	Stack based buffer overflow in Ipswitch IMail server up to and including 12.5.5 allows remote attackers to execute arbitrary code via unspecified vectors in IMmailSrv, aka ETBL or ETCETERABLUE. CVE ID: CVE-2017-12638	https://docs.ipswitch.com/_Messaging/IMailServer/v12.5.6/ReleaseNotes/index.htm#link8	A-IPS-IMAIL-161017/64						
Jaspersoft											
Jasperreports											
Gain Information	01-10-2017	4	Jaspersoft JasperReports 4.7 suffers from a saved credential disclosure vulnerability, which allows a remote authenticated user to retrieve stored Data Source passwords by accessing flow.html and reading the HTML source code of the page reached in an Edit	https://github.com/binary1985/VulnerabilityDisclosure/blob/master/JasperSoft%20JasperReports%20-%204.7%20-	A-JAS-JASPE-161017/65						
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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			action for a Data Source connector. CVE ID: CVE-2017-14941	%20CVE-2017-14941	

Jenkins

Blue Ocean

NA	04-10-2017	4	Blue Ocean allows the creation of GitHub organization folders that are set up to scan a GitHub organization for repositories and branches containing a Jenkinsfile, and create corresponding pipelines in Jenkins. It did not properly check the current user's authentication and authorization when configuring existing GitHub organization folders. This allowed users with read access to the GitHub organization folder to reconfigure it, including changing the GitHub API endpoint for the organization folder to an attacker-controlled server to obtain the GitHub access token, if the organization folder was initially created using Blue Ocean. CVE ID: CVE-2017-1000110	https://jenkins.io/security/advisory/2017-08-07/	A-JEN-BLUE - 161017/67
----	------------	---	--	---	------------------------

Config File Provider

NA	04-10-2017	4	The Config File Provider Plugin is used to centrally manage configuration files that often include secrets, such as passwords. Users with only Overall/Read access to Jenkins were able to access URLs directly that allowed viewing these files. Access to view these files now requires sufficient permissions to configure the provided files, view the configuration of the folder in which the configuration files are defined, or have Job/Configure permissions to a job able to use these files. CVE ID: CVE-2017-1000104	https://jenkins.io/security/advisory/2017-08-07/	A-JEN-CONFI-161017/68
----	------------	---	--	---	-----------------------

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
Script Security					
NA	04-10-2017	4	The default whitelist included the following unsafe entries: DefaultGroovyMethods.putAt(Object, String, Object); DefaultGroovyMethods.getAt(Object, String). These allowed circumventing many of the access restrictions implemented in the script sandbox by using e.g. currentBuild['rawBuild'] rather than currentBuild.rawBuild. Additionally, the following entries allowed accessing private data that would not be accessible otherwise due to script security: groovy.json.JsonOutput.toJson(Closure);groovy.json.JsonOutput.toJson(Object). CVE ID: CVE-2017-100095	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-SCRIP-161017/69
Docker Commons					
Gain Information	04-10-2017	4	Docker Commons Plugin provides a list of applicable credential IDs to allow users configuring a job to select the one they'd like to use to authenticate with a Docker Registry. This functionality did not check permissions, allowing any user with Overall/Read permission to get a list of valid credentials IDs. Those could be used as part of an attack to capture the credentials using another vulnerability. CVE ID: CVE-2017-100094	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-DOCKE-161017/70
Datadog					
XSS Gain Information	04-10-2017	4.3	The Datadog Plugin stores an API key to access the Datadog service in the global Jenkins configuration. While the API key is stored encrypted on disk, it was transmitted in plain text as part of the configuration form. This could	https://jenkins.io/security/advisory/2017-08-07/	A-JEN-DATAD-161017/71

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			result in exposure of the API key for example through browser extensions or cross-site scripting vulnerabilities. The Datadog Plugin now encrypts the API key transmitted to administrators viewing the global configuration form. CVE ID: CVE-2017-1000114		
Blue Ocean					
NA	04-10-2017	5	The optional Run/Artifacts permission can be enabled by setting a Java system property. Blue Ocean did not check this permission before providing access to archived artifacts, Item/Read permission was sufficient. CVE ID: CVE-2017-1000105	https://jenkins.io/security/advisory/2017-08-07/	A-JEN-BLUE-161017/72
Pipeline					
NA	04-10-2017	5	Builds in Jenkins are associated with an authentication that controls the permissions that the build has to interact with other elements in Jenkins. The Pipeline: Build Step Plugin did not check the build authentication it was running as and allowed triggering any other project in Jenkins. CVE ID: CVE-2017-1000089	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-PIPEL-161017/73
Execute Code	04-10-2017	6.5	Arbitrary code execution due to incomplete sandbox protection: Constructors, instance variable initializers, and instance initializers in Pipeline scripts were not subject to sandbox protection, and could therefore execute arbitrary code. This could be exploited e.g. by regular Jenkins users with the permission to configure Pipelines in Jenkins, or by trusted committers to repositories containing Jenkinsfiles. CVE ID: CVE-2017-1000096	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-PIPEL-161017/74

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Poll Scm											
CSRF	04-10-2017	6.8	Poll SCM Plugin was not requiring requests to its API be sent via POST, thereby opening itself to Cross-Site Request Forgery attacks. This allowed attackers to initiate polling of projects with a known name. While Jenkins in general does not consider polling to be a protection-worthy action as it's similar to cache invalidation, the plugin specifically adds a permission to be able to use this functionality, and this issue undermines that permission. CVE ID: CVE-2017-100093	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-POLL-161017/75						
Github Branch Source											
CSRF	04-10-2017	6.8	GitHub Branch Source Plugin connects to a user-specified GitHub API URL (e.g. GitHub Enterprise) as part of form validation and completion (e.g. to verify Scan Credentials are correct). This functionality improperly checked permissions, allowing any user with Overall/Read access to Jenkins to connect to any web server and send credentials with a known ID, thereby possibly capturing them. Additionally, this functionality did not require POST requests be used, thereby allowing the above to be performed without direct access to Jenkins via Cross-Site Request Forgery. CVE ID: CVE-2017-100091	https://jenkins.io/security/advisory/2017-07-10/	A-JEN-GITHU-161017/76						
Lame Project											
Lame											
Overflow	06-10-2017	4.3	LAME 3.99.5 has a stack-based buffer overflow in <code>unpack_read_samples</code> in <code>frontend/get_audio.c</code> , a different	https://sourceforge.net/p/lame/bugs/479/	A-LAM-LAME-161017/77						
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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			vulnerability than CVE-2017-9412. CVE ID:CVE-2017-15046		
Overflow	06-10-2017	4.3	LAME 3.99.5 has a heap-based buffer over-read in fill_buffer in libmp3lame/util.c, related to lame_encode_buffer_sample_t in libmp3lame/lame.c, a different vulnerability than CVE-2017-9410. CVE ID: CVE-2017-15045	https://sourceforge.net/p/lame/bugs/478/	A-LAM-LAME-161017/78
Overflow	04-10-2017	4.3	LAME 3.99.5 has a heap-based buffer over-read when handling a malformed file in k_34_4 in vbrquantize.c. CVE ID: CVE-2017-15018	https://sourceforge.net/p/lame/bugs/480/	A-LAM-LAME-161017/79
NA	04-10-2017	6.8	LAME 3.99.5 has a NULL Pointer Dereference in the hip_decode_init function within libmp3lame/mpglib_interface.c via a malformed mpg file, because of an incorrect calloc call. CVE ID:CVE-2017-15019	https://sourceforge.net/p/lame/bugs/477/	A-LAM-LAME-161017/80

Lenovo

System Update

Gain Privileges	02-10-2017	7.2	Lenovo System Update (formerly ThinkVantage System Update) before 5.07.0013 allows local users to submit commands to the System Update service (SUService.exe) and gain privileges by launching signed Lenovo executables. CVE ID:CVE-2015-6971	https://support.lenovo.com/us/en/product_security/lsu_privilege	A-LEN-SYSTE-161017/81
-----------------	------------	-----	---	---	-----------------------

Fingerprint Manager

Gain Privileges	02-10-2017	7.2	Services and files in Lenovo Fingerprint Manager before 8.01.42 have incorrect ACLs, which allows local users to invalidate local checks and gain privileges via standard filesystem operations. CVE ID:CVE-2015-3321	https://support.lenovo.com/us/en/product_security/lenovo_fpr	A-LEN-FINGE-161017/82
-----------------	------------	-----	---	---	-----------------------

Libcsoap Project

Libcsoap

DoS	06-10-2017	5	nanohhttp in libcsoap allows remote	http://www.ope	A-LIB-
-----	------------	---	-------------------------------------	---	--------

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):
 CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Authorization header. CVE ID: CVE-2015-2297	nwall.com/lists/oss-security/2015/03/15/4	LIBCS-161017/83
Mercurial					
<i>Mercurial</i>					
NA	04-10-2017	5	Mercurial prior to version 4.3 is vulnerable to a missing symlink check that can malicious repositories to modify files outside the repository CVE ID: CVE-2017-1000115	https://www.mercurial-scm.org/wiki/W hatsNew#Mercurial_4.3_2F_4.3.1_282017-08-10.29	A-MER-MERCU-161017/84
NA	04-10-2017	7.5	Mercurial prior to 4.3 did not adequately sanitize hostnames passed to ssh, leading to possible shell-injection attacks. CVE ID: CVE-2017-1000116	https://www.mercurial-scm.org/wiki/W hatsNew#Mercurial_4.3_2F_4.3.1_282017-08-10.29	A-MER-MERCU-161017/85
Nexusphp Project					
<i>Nexusphp</i>					
XSS CSRF	02-10-2017	4.3	Multiple cross-site request forgery (CSRF) vulnerabilities in NexusPHP 1.5 allow remote attackers to hijack the authentication of administrators for requests that conduct cross-site scripting (XSS) attacks via the (1) linkname, (2) url, or (3) title parameter in an add action to linksmanage.php. CVE ID: CVE-2017-12792	https://github.com/UUUUnotfoun d/cve-2017-12792	A-NEX-NEXUS-161017/86
Openexr					
<i>Openexr</i>					
DoS	02-10-2017	4.3	Header::readfrom in llmImf/ImfHeader.cpp in OpenEXR 2.2.0 allows remote attackers to cause a denial of service (excessive memory allocation) via a crafted file that is accessed with the ImfOpenInputFile function in	https://github.com/openexr/openexr/issues/248	A-OPE-OPENE-161017/87

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			llmImf/ImfCRgbaFile.cpp. CVE ID: CVE-2017-14988		
Openkm					
<i>Openkm</i>					
XSS	06-10-2017	3.5	Cross-site scripting (XSS) vulnerability in OpenKM before 6.4.19 allows remote authenticated users to inject arbitrary web script or HTML via the Tasks parameter. CVE ID: CVE-2014-8957	NA	A-OPE-OPENK-161017/88
Opentext					
<i>Document Sciences Xpression</i>					
XSS	02-10-2017	4.3	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to Cross-Site Scripting: /xAdmin/html/Deployment (cat_id). CVE ID: CVE-2017-14756	NA	A-OPE-DOCUM-161017/89
XSS	02-10-2017	4.3	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to Cross-Site Scripting: /xAdmin/html/XPressoDoc, parameter: categoryId. CVE ID: CVE-2017-14755	NA	A-OPE-DOCUM-161017/90
Sql	02-10-2017	6.5	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to SQL Injection: /xAdmin/html/cm_doclist_view_uc.jsp, parameter: documentId. In order for this vulnerability to be exploited, an attacker must authenticate to the application first. CVE ID: CVE-2017-14758	NA	A-OPE-DOCUM-161017/91

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sql	02-10-2017	6.5	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to SQL Injection: /xDashboard/html/jobhistory/downloadSupportFile.action, parameter: jobRunId. In order for this vulnerability to be exploited, an attacker must authenticate to the application first. CVE ID: CVE-2017-14757	NA	A-OPE-DOCUM-161017/92
Dir. Trav.	02-10-2017	6.8	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to Arbitrary File Read: /xAdmin/html/cm_datasource_group_xsd.jsp, parameter: xsd_datasource_schema_file filename. In order for this vulnerability to be exploited, an attacker must authenticate to the application first. CVE ID: CVE-2017-14754	NA	A-OPE-DOCUM-161017/93
DoS	02-10-2017	7.5	OpenText Document Sciences xPression (formerly EMC Document Sciences xPression) v4.5SP1 Patch 13 (older versions might be affected as well) is prone to an XML External Entity vulnerability: /xFramework/services/QuickDoc.QuickDocHttpSoap11Endpoint/. An unauthenticated user is able to read directory listings or system files, or cause SSRF or Denial of Service. CVE ID: CVE-2017-14759	NA	A-OPE-DOCUM-161017/94

Openvpn

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID					
Openvpn										
Exec Code Overflow	03-10-2017	6.8	OpenVPN versions before 2.3.3 and 2.4.x before 2.4.4 are vulnerable to a buffer overflow vulnerability when key-method 1 is used, possibly resulting in code execution. CVE ID: CVE-2017-12166	NA	A-OPE-OPENV-161017/95					
Openvswitch										
Openvswitch										
NA	01-10-2017	5	In lib/ofp-util.c in Open vSwitch (OvS) before 2.8.1, there are multiple memory leaks while parsing malformed OpenFlow group mod messages. NOTE: the vendor disputes the relevance of this report, stating "it can only be triggered by an OpenFlow controller, but OpenFlow controllers have much more direct and powerful ways to force Open vSwitch to allocate memory, such as by inserting flows into the flow table." CVE ID: CVE-2017-14970	https://mail.openvswitch.org/pipermail/ovs-dev/2017-September/339086.html	A-OPE-OPENV-161017/96					
Paessler										
Prtg Network Monitor										
XSS	03-10-2017	3.5	PRTG Network Monitor version 17.3.33.2830 is vulnerable to stored Cross-Site Scripting on all sensor titles, related to incorrect error handling for a %00 in the SRC attribute of an IMG element. CVE-2017-15008	https://medium.com/stolabs/security-issue-on-prtg-network-manager-ada65b45d37b	A-PAE-PRTG-161017/97					
XSS	03-10-2017	4.3	PRTG Network Monitor version 17.3.33.2830 is vulnerable to reflected Cross-Site Scripting on error.htm (the error page), via the errmsg parameter. CVE ID: CVE-2017-15009	https://medium.com/stolabs/security-issue-on-prtg-network-manager-ada65b45d37b	A-PAE-PRTG-161017/98					
Phpbugtracker Project										
Phpbugtracker										
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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
XSS	06-10-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Issuetracker phpBugTracker before 1.7.2 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters. CVE ID: CVE-2015-2148	http://www.opennwall.com/lists/oss-security/2015/02/28/1	A-PHP-PHPBU-161017/99
XSS	06-10-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow remote attackers to inject arbitrary web script or HTML via unspecified parameters. CVE ID: CVE-2015-2145	http://www.opennwall.com/lists/oss-security/2015/02/28/1	A-PHP-PHPBU-161017/100
XSS	06-10-2017	3.5	Multiple cross-site scripting (XSS) vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow remote authenticated users to inject arbitrary web script or HTML via the (1) project name parameter to project.php; the (2) use_js parameter to user.php; the (3) use_js parameter to group.php; the (4) Description parameter to status.php; the (5) Description parameter to severity.php; the (6) Regex parameter to os.php; or the (7) Name parameter to database.php. CVE ID: CVE-2015-2144	https://github.com/a-v-k/phpBugTracker/issues/4	A-PHP-PHPBU-161017/101
CSRF	06-10-2017	6	Multiple cross-site request forgery (CSRF) vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow remote authenticated users to (1) hijack the authentication of users for requests that cause an unspecified impact via the id parameter to project.php, (2) hijack the authentication of users for requests that cause an unspecified impact via the group_id parameter to group.php, (3) hijack	https://github.com/a-v-k/phpBugTracker/issues/4	A-PHP-PHPBU-161017/102

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the authentication of users for requests that delete statuses via the status_id parameter to status.php, (4) hijack the authentication of users for requests that delete severities via the severity_id parameter to severity.php, (5) hijack the authentication of users for requests that cause an unspecified impact via the priority_id parameter to priority.php, (6) hijack the authentication of users for requests that delete the operating system via the os_id parameter to os.php, (7) hijack the authentication of users for requests that delete databases via the database_id parameter to database.php, or (8) hijack the authentication of users for requests that delete sites via the site_id parameter to sites.php. CVE ID: CVE-2015-2142		
CSRF	06-10-2017	6.8	Multiple cross-site request forgery (CSRF) vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow remote attackers to hijack the authentication of users for requests that cause an unspecified impact via unknown parameters. CVE ID: CVE-2015-2143	http://www.opnwall.com/lists/oss-security/2015/02/28/1	A-PHP-PHPBU-161017/103
Execute Code Sql	06-10-2017	7.5	Multiple SQL injection vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow remote attackers to execute arbitrary SQL commands via unspecified parameters. CVE ID: CVE-2015-2147	NA	A-PHP-PHPBU-161017/104
Execute Code Sql	06-10-2017	7.5	Multiple SQL injection vulnerabilities in Issuetracker phpBugTracker before 1.7.0 allow	https://github.com/a-v-k/phpBugTracke	A-PHP-PHPBU-161017/1

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to execute arbitrary SQL commands via the (1) id parameter to project.php, the (2) group_id parameter to group.php, the (3) status_id parameter to status.php, the (4) resolution_id parameter to resolution.php, the (5) severity_id parameter to severity.php, the (6) priority_id parameter to priority.php, the (7) os_id parameter to os.php, or the (8) site_id parameter to site.php. CVE ID: CVE-2015-2146	r/issues/4	05

Phpcollab

Phpcollab

Execute Code	02-10-2017	6.5	Unrestricted file upload vulnerability in clients/editclient.php in PhpCollab 2.5.1 and earlier allows remote authenticated users to execute arbitrary code by uploading a file with an executable extension, then accessing it via a direct request to the file in logos_clients/. CVE ID: CVE-2017-6090	NA	A-PHP-PHPCO-161017/106
Execute Code Sql	02-10-2017	7.5	SQL injection vulnerability in PhpCollab 2.5.1 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) project or id parameters to topics/deletetopics.php; the (2) id parameter to bookmarks/deletebookmarks.php; or the (3) id parameter to calendar/deletecalendar.php. CVE ID: CVE-2017-6089	NA	A-PHP-PHPCO-161017/107

Pivotx

Pivotx

Execute Code	01-10-2017	6.5	lib.php in PivotX 2.3.11 does not properly block uploads of dangerous file types by admin	https://sourceforge.net/p/pivot-weblog/code/44	A-PIV-PIVOT-161017/1
--------------	------------	-----	---	---	----------------------

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users, which allows remote PHP code execution via an upload of a .php file. CVE ID: CVE-2017-14958	90/	08

PI32

Photoline

Execute Code Overflow Mem. Corr.	05-10-2017	6.8	A memory corruption vulnerability exists in the .TGA parsing functionality of Computerinsel Photoline 20.02. A specially crafted .TGA file can cause an out of bounds write resulting in potential code execution. An attacker can send a specific .TGA file to trigger this vulnerability. CVE ID: CVE-2017-12106	NA	A-PL3-PHOTO-161017/109
Execute Code Overflow Mem. Corr.	05-10-2017	6.8	An memory corruption vulnerability exists in the .SVG parsing functionality of Computerinsel Photoline 20.02. A specially crafted .SVG file can cause a vulnerability resulting in memory corruption, which can potentially lead to arbitrary code execution. An attacker can send a specific .SVG file to trigger this vulnerability. CVE ID: CVE-2017-2920	https://github.com/libofx/libofx/commit/a70934eea95c76a7737b83773bffe8738935082d	A-PL3-PHOTO-161017/110
Execute Code Overflow Mem. Corr.	05-10-2017	6.8	An memory corruption vulnerability exists in the .GIF parsing functionality of Computerinsel Photoline 20.02. A specially crafted .GIF file can cause a vulnerability resulting in potential code execution. An attacker can send specific .GIF file to trigger this vulnerability. CVE ID: CVE-2017-2880	NA	A-PL3-PHOTO-161017/111

Qnap

Qts Helpdesk

Sql Gain Information	06-10-2017	5	QNAP has already patched this vulnerability. This security concern allows a remote attacker to	https://www.qnap.com/en/security-	A-QNA-QTS H-161017/1
----------------------	------------	---	--	---	----------------------

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			perform an SQL injection on the application and obtain Helpdesk application information. A remote attacker does not require any privileges to successfully execute this attack. CVE ID: CVE-2017-13068	advisory/nas-201709-29	12

Rapid7

Metasploit

CSRF	06-10-2017	4.3	The web UI in Rapid7 Metasploit before 4.14.1-20170828 allows logout CSRF, aka R7-2017-22. CVE ID: CVE-2017-15084	https://blog.rapid7.com/2017/10/06/vulnerabilities-affecting-four-rapid7-products-fixed/	A-RAP-METAS-161017/113
------	------------	-----	---	---	------------------------

Skyboxsecurity

Skybox Manager Client Application

Gain Information	02-10-2017	2.1	Skybox Manager Client Application is prone to information disclosure via a username enumeration attack. A local unauthenticated attacker could exploit the flaw to obtain valid usernames, by analyzing error messages upon valid and invalid account login attempts. CVE ID: CVE-2017-14772	https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Product_Security_Advisory_9_28_17.pdf	A-SKY-SKYBO-161017/115
Gain Information	02-10-2017	2.1	Skybox Manager Client Application prior to 8.5.501 is prone to an information disclosure vulnerability of user password hashes. A local authenticated attacker can access the password hashes in a debugger-pause state during the authentication process. CVE-2017-14770	https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Product_Security_Advisory_9_28_17.pdf	A-SKY-SKYBO-161017/116
NA	02-10-2017	3.6	Skybox Manager Client Application prior to 8.5.501 is prone to an arbitrary file upload vulnerability due to insufficient input validation of user-supplied files path when uploading files via the application.	https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Product_Security_Advisory_9_28_17.pdf	A-SKY-SKYBO-161017/117

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			During a debugger-pause state, a local authenticated attacker can upload an arbitrary file and overwrite existing files within the scope of the affected application. CVE ID: CVE-2017-14771	_28_17.pdf	
NA	02-10-2017	4.6	Skybox Manager Client Application prior to 8.5.501 is prone to an elevation of privileges vulnerability during authentication of a valid user in a debugger-pause state. The vulnerability can only be exploited by a local authenticated attacker. CVE ID: CVE-2017-14773	https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox_Product_Security_Advisory_9_28_17.pdf	A-SKY-SKYBO-161017/118
Solarwinds					
Network Performance Monitor					
XSS	02-10-2017	3.5	Persistent cross-site scripting (XSS) in the Add Node function of SolarWinds Network Performance Monitor version 12.0.15300.90 allows remote attackers to introduce arbitrary JavaScript into various vulnerable parameters. CVE ID: CVE-2017-9537	NA	A-SOL-NETWO-161017/119
Tech-banker					
Gallery Bank					
XSS	06-10-2017	4.3	Cross-site scripting (XSS) vulnerability in Best Gallery Albums Plugin before 3.0.70 for WordPress allows remote attackers to inject arbitrary web script or HTML via the order_id parameter in the gallery_album_sorting page to wp-admin/admin.php. CVE ID: CVE-2014-8758	NA	A-TEC-GALLE-161017/120
Trendmicro					
Officescan					
NA	05-10-2017	5	A Host Header Injection vulnerability in Trend Micro OfficeScan XG (12.0) may allow an attacker to spoof a particular Host header, allowing the attacker to	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/121

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			render arbitrary links that point to a malicious website with poisoned Host header webpages. CVE ID: CVE-2017-14087		
NA	05-10-2017	5	A vulnerability in Trend Micro OfficeScan 11.0 and XG allows remote unauthenticated users who can access the system to download the OfficeScan encryption file. CVE ID: CVE-2017-14083	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/122
Gain Information	05-10-2017	6.4	Information disclosure vulnerabilities in Trend Micro OfficeScan 11.0 and XG may allow unauthenticated users who can access the OfficeScan server to query the network's NT domain or the PHP version and modules. CVE ID: CVE-2017-14085	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/123
Execute Code	05-10-2017	6.8	A potential Man-in-the-Middle (MitM) attack vulnerability in Trend Micro OfficeScan 11.0 and XG may allow attackers to execute arbitrary code on vulnerable installations. CVE ID: CVE-2017-14084	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/124
Execute Code Overflow Mem. Corr.	05-10-2017	6.9	Memory Corruption Privilege Escalation vulnerabilities in Trend Micro OfficeScan 11.0 and XG allows local attackers to execute arbitrary code and escalate privileges to resources normally reserved for the kernel on vulnerable installations by exploiting tmwfp.sys. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit the vulnerability. CVE ID: CVE-2017-14088	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/125
Overflow Mem. Corr.	05-10-2017	7.5	An Unauthorized Memory Corruption vulnerability in Trend Micro OfficeScan 11.0 and XG may	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/1

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			allow remote unauthenticated users who can access the OfficeScan server to target cgiShowClientAdm.exe and cause memory corruption issues. CVE ID: CVE-2017-14089		26
NA	05-10-2017	7.8	Pre-authorization Start Remote Process vulnerabilities in Trend Micro OfficeScan 11.0 and XG may allow unauthenticated users who can access the OfficeScan server to start the fcgiOfcDDA.exe executable or cause a potential INI corruption, which may cause the server disk space to be consumed with dump files from continuous HTTP requests. CVE ID: CVE-2017-14086	https://success.trendmicro.com/solution/1118372	A-TRE-OFFIC-161017/127

Udesign Project

Udesign

XSS	02-10-2017	4.3	Cross-site scripting (XSS) vulnerability in the uDesign (aka U-Design) theme 2.3.0 before 2.7.10 for WordPress allows remote attackers to inject arbitrary web script or HTML via a fragment identifier, as demonstrated by #<svg onload=alert(1)>. CVE ID: CVE-2015-7357	http://themeforest.net/item/ude-sign-responsive-wordpress-theme/253220	A-UDE-UDESI-161017/128
-----	------------	-----	--	---	------------------------

Wireshark

Wireshark

NA	2017-10-10	5	In Wireshark 2.4.0 to 2.4.1, 2.2.0 to 2.2.9, and 2.0.0 to 2.0.15, the DMP dissector could crash. This was addressed in epan/dissectors/packet-dmp.c by validating a string length. CVE ID: CVE-2017-15191	https://www.wireshark.org/security/wnpa-sec-2017-44.html	A-WIR-WIRES-161017/129
NA	2017-10-10	7.8	In Wireshark 2.4.0 to 2.4.1 and 2.2.0 to 2.2.9, the MBIM dissector could crash or exhaust system memory. This was addressed in	https://www.wireshark.org/security/wnpa-sec-2017-43.html	A-WIR-WIRES-161017/130

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID						
			epan/dissectors/packet-mbim.c by changing the memory-allocation approach. CVE ID: CVE-2017-15193								
Wolfssl											
Wolfssl											
NA	06-10-2017	4.3	CyaSSL does not check the key usage extension in leaf certificates, which allows remote attackers to spoof servers via a crafted server certificate not authorized for use in an SSL/TLS handshake. CVE ID: CVE-2014-2903	http://www.openssl.org/news/secadv_20140418/2	A-WOL-WOLFS-161017/131						
Wordpress											
Wordpress											
Sql Gain Information	02-10-2017	4	WordPress 4.8.2 stores cleartext wp_signups.activation_key values (but stores the analogous wp_users.user_activation_key values as hashes), which might make it easier for remote attackers to hijack unactivated user accounts by leveraging database read access (such as access gained through an unspecified SQL injection vulnerability). CVE ID: CVE-2017-14990	NA	A-WOR-WORDP-161017/132						
WPA;Wpa2											
WPA/Wpa2											
NA	2017-10-16	5.4	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the pairwise key in the four-way handshake. CVE ID: CVE-2017-13077	NA	A-WPA-WPA/W-161017/133						
Wpmudev											
Smush Image Compression And Optimization											
Dir. Trav.	06-10-2017	5	The Smush Image Compression and Optimization plugin before 2.7.6 for WordPress allows directory traversal. CVE ID: CVE-2017-15079	https://wordpress.org/support/topic/file-transversal-bug/	A-WPM-SMUSH-161017/134						
OPERATING SYSTEM(OS)											
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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID						
Cisco											
<i>Ios Xr</i>											
DoS Overflow	05-10-2017	5	A vulnerability in the gRPC code of Cisco IOS XR Software for Cisco Network Convergence System (NCS) 5500 Series Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition when the emsd service stops. The vulnerability is due to the software's inability to process HTTP/2 packets. An attacker could exploit this vulnerability by sending a malformed HTTP/2 frame to the affected device. A successful exploit could allow the attacker to create a DoS condition when the emsd service stops. Cisco Bug IDs: CSCvb99388. CVE ID: CVE-2017-12270	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20171004-ncs	O-CIS-IOX-161017/135						
Freebsd											
<i>Freebsd</i>											
NA	05-10-2017	6.8	In FreeBSD through 11.1, the smb_strdupin function in sys/netsmb/smb_subr.c has a race condition with a resultant out-of-bounds read, because it can cause t2p->t_name strings to lack a final '\0' character. CVE ID: CVE-2017-15037	https://svnweb.freebsd.org/base?view=revision&revision=324102	O-FRE-FREEB-161017/136						
Google											
<i>Android</i>											
Gain Information	03-10-2017	4.3	An information disclosure vulnerability in the Android media framework (libeffects). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63662938. CVE ID: CVE-2017-0816	https://android.googlesource.com/platform/frameworks/av/+f490fc335772a9b14e78997486f4a572b0594c04	O-GOO-ANDRO-161017/137						
Gain Information	03-10-2017	4.3	An information disclosure vulnerability in the Android media	https://android.googlesource.com	O-GOO-ANDRO-						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			framework (libeffects). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63526567. CVE ID: CVE-2017-0815	m/platform/frameworks/av/+/f490fc335772a9b14e78997486f4a572b0594c04	161017/138
Gain Information	03-10-2017	5	An information disclosure vulnerability in the Broadcom wifi driver. Product: Android. Versions: Android kernel. Android ID: A-37305633. References: B-V2017063002. CVE ID: CVE-2017-0825	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/139
Gain Information	03-10-2017	5	An information disclosure vulnerability in the Android system (rild). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37896655. CVE ID: CVE-2017-0823	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/140
Gain Information	03-10-2017	5	An information disclosure vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63522430. CVE ID: CVE-2017-0817	https://android.googlesource.com/platform/frameworks/av/+/d834160d9759f1098df692b34e6eeb548f9e317b	O-GOO-ANDRO-161017/141
DoS	03-10-2017	5	A denial of service vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 7.0, 7.1.1, 7.1.2. Android ID: A-36531046. CVE ID: CVE-2017-0813	https://android.googlesource.com/platform/frameworks/av/+/7fa3f552a6f34ed05c15e64ea30b8eed53f77a41	O-GOO-ANDRO-161017/142
Gain Information	03-10-2017	5	An information disclosure vulnerability in the Android framework (file system). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62301183. CVE ID: CVE-2017-0808	https://android.googlesource.com/platform/libcore/+/809681f310663288e83587089abb7715c68f6924	O-GOO-ANDRO-161017/143
NA	03-10-2017	7.5	An elevation of privilege vulnerability in the Motorola	https://source.android.com/secu	O-GOO-ANDRO-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			bootloader. Product: Android. Versions: Android kernel. Android ID: A-62345044. CVE ID: CVE-2017-0829	rity/bulletin/pixel/01-10-2017	161017/144
NA	03-10-2017	7.5	An elevation of privilege vulnerability in the Huawei bootloader. Product: Android. Versions: Android kernel. Android ID: A-34622855. CVE ID: CVE-2017-0828	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/145
NA	03-10-2017	7.5	An elevation of privilege vulnerability in the Broadcom wifi driver. Product: Android. Versions: Android kernel. Android ID: A-37622847. References: B-V2017063001. CVE-2017-0824	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/146
NA	03-10-2017	7.5	An elevation of privilege vulnerability in the Android system (camera). Product: Android. Versions: 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63787722. CVE ID: CVE-2017-0822	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/147
NA	03-10-2017	7.8	A vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62187433. CVE ID: CVE-2017-0820	https://android.googlesource.com/platform/frameworks/av/+8a3a2f6ea7def1a81bb32b3c9f3537f84749b9d	O-GOO-ANDRO-161017/148
NA	03-10-2017	7.8	A vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63045918. CVE ID: CVE-2017-0819	https://android.googlesource.com/platform/external/libhevc/+87fb7909c49e6a4510ba86ace1ffc83459c7e1b9	O-GOO-ANDRO-161017/149
NA	03-10-2017	7.8	A vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-63581671. CVE ID: CVE-2017-0818	https://android.googlesource.com/platform/frameworks/av/+d07f5c14e811951ff9b411ceb84e	O-GOO-ANDRO-161017/150

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				7288e0d04aaf	
NA	03-10-2017	7.8	An information disclosure vulnerability in the Android media framework (n/a). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62800140. CVE ID: CVE-2017-0814	https://android.googlesource.com/platform/external/tremolo/+eeb4e45d5683f88488c083ecf142dc89bc3f0b47	O-GOO-ANDRO-161017/151
NA	03-10-2017	9.3	An elevation of privilege vulnerability in the MediaTek soc driver. Product: Android. Versions: Android kernel. Android ID: A-62539960. References: M-ALPS03353876, M-ALPS03353861, M-ALPS03353869, M-ALPS03353867, M-ALPS03353872. CVE ID: CVE-2017-0827	https://source.android.com/security/bulletin/01-10-2017	O-GOO-ANDRO-161017/152
NA	03-10-2017	9.3	An elevation of privilege vulnerability in the HTC bootloader. Product: Android. Versions: Android kernel. Android ID: A-34949781. CVE ID: CVE-2017-0826	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/153
NA	03-10-2017	9.3	An elevation of privilege vulnerability in the Android media framework (audio hal). Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62873231. CVE ID: CVE-2017-0812	https://android.googlesource.com/device/google/dragon/+7df7ec13b1d222ac3a66797fbc432605ea8f973f	O-GOO-ANDRO-161017/154
Execute Code	03-10-2017	9.3	A remote code execution vulnerability in the Android media framework (libhevc). Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-37930177. CVE ID: CVE-2017-0811	https://android.googlesource.com/platform/external/libhevc/+25c0ffbe6a181b4a373c3c9b421ea449d457e6ed	O-GOO-ANDRO-161017/155
Execute Code	03-10-2017	9.3	A remote code execution vulnerability in the Android media framework (libmpeg2). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-	https://android.googlesource.com/platform/external/libmpeg2/+7737780815fe5	O-GOO-ANDRO-161017/156

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			38207066. CVE ID: CVE-2017-0810	23ad7b0e49456 eb75d27a30818 a	
Execute Code	03-10-2017	9.3	A remote code execution vulnerability in the Android media framework (libstagefright). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62673128. CVE ID: CVE-2017-0809	https://android.googlesource.com/platform/frameworks/av/+552a3b5df2a6876d10da20f72e4cc0d44ac2c790	O-GOO-ANDRO-161017/157
NA	03-10-2017	9.3	An elevation of privilege vulnerability in the Android framework (gatekeeperresponse). Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2, 8.0. Android ID: A-62998805. CVE ID: CVE-2017-0806	https://source.android.com/security/bulletin/01-10-2017	O-GOO-ANDRO-161017/158
NA	03-10-2017	10	An elevation of privilege vulnerability in the Android framework (ui framework). Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-35056974. CVE ID: CVE-2017-0807	https://source.android.com/security/bulletin/pixel/01-10-2017	O-GOO-ANDRO-161017/159

Linux

Linux Kernel

Bypass Gain Information	01-10-2017	2.1	The waitid implementation in kernel/exit.c in the Linux kernel through 4.13.4 accesses rusage data structures in unintended cases, which allows local users to obtain sensitive information, and bypass the KASLR protection mechanism, via a crafted system call. CVE ID: CVE-2017-14954	NA	O-LIN-LINUX-161017/160
Gain Information	03-10-2017	2.1	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel before 4.13.4 allows local users to obtain sensitive information from uninitialized kernel heap-memory locations via an SG_GET_REQUEST_TABLE ioctl	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3e0097499839e0fe3af380410eababe5a4	O-LIN-LINUX-161017/161

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCHIPC ID
			call for /dev/sg0. CVE ID: CVE-2017-14991	7c4cf9	

Loytec

Lvis-3me Firmware

XSS	05-10-2017	4.3	A Cross-site Scripting issue was discovered in LOYTEC LVIS-3ME versions prior to 6.2.0. The web interface lacks proper web request validation, which could allow XSS attacks to occur if an authenticated user of the web interface is tricked into clicking a malicious link. CVE ID: CVE-2017-13994	NA	O-LOY-LVIS--161017/162
NA	05-10-2017	6	An Insufficiently Protected Credentials issue was discovered in LOYTEC LVIS-3ME versions prior to 6.2.0. The application does not sufficiently protect sensitive information from unauthorized access. CVE ID: CVE-2017-13998	NA	O-LOY-LVIS--161017/163
Execute Code Dir. Trav.	05-10-2017	6.5	A Relative Path Traversal issue was discovered in LOYTEC LVIS-3ME versions prior to 6.2.0. The web user interface fails to prevent access to critical files that non administrative users should not have access to, which could allow an attacker to create or modify files or execute arbitrary code. CVE ID: CVE-2017-13996	NA	O-LOY-LVIS--161017/164
Execute Code	05-10-2017	6.8	An Insufficient Entropy issue was discovered in LOYTEC LVIS-3ME versions prior to 6.2.0. The application does not utilize sufficiently random number generation for the web interface authentication mechanism, which could allow remote code execution. CVE ID: CVE-2017-13992	NA	O-LOY-LVIS--161017/165

OS;Application (OS/A)

Canonical;Debian;Fedoraproject;Novell;Redhat/Thekelleys

Ubuntu Linux/Debian Linux/Fedora/Leap/Enterprise Linux Desktop;Enterprise Linux

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server;Enterprise Linux Workstation/Dnsmasq					
NA	02-10-2017	5	In dnsmasq before 2.78, if the DNS packet size does not match the expected size, the size parameter in a memset call gets a negative value. As it is an unsigned value, memset ends up writing up to 0xffffffff zero's (0xffffffffffffff in 64 bit platforms), making dnsmasq crash. CVE ID: CVE-2017-13704	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/166
DoS	02-10-2017	7.8	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request. CVE ID: CVE-2017-14496	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/167
Gain Information	02-10-2017	4.3	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests. CVE ID: CVE-2017-14494	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/168
DoS	02-10-2017	5	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation. CVE ID: CVE-2017-14495	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/169
DoS Execute Code Overflow	02-10-2017	7.5	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request. CVE ID: CVE-2017-14493	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/170
DoS Execute Code	02-10-2017	7.5	Heap-based buffer overflow in dnsmasq before 2.78 allows remote	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request. CVE ID: CVE-2017-14492	y/vulnerabilities/3199382	161017/171
DoS Execute Code Overflow	03-10-2017	7.5	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response. CVE ID: CVE-2017-14491	https://access.redhat.com/security/vulnerabilities/3199382	O-CAN-UBUNT-161017/172

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): CSRF-Cross Site Request Forgery; Dir. Trav.-Directory Traversal; DoS-Denial of Service; NA- Not Applicable; Sql-SQL Injection; XSS-Cross Site Scripting;										