National Critical Information Infrastructure Protection Centre

CVE Report

CV Scoring Scale : 3-10   01-31 Mar 2018   Vol. 05 No.06

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
Application					
Adminer					
Adminer					
NA	05-03-2018	7.5	Adminer through 4.3.1 has SSRF via the server parameter. **CVE ID : CVE-2018-7667**	NA	A-ADM-ADMIN-20418/1
Advantig					
Dualdesk					
DoS	03-03-2018	5	Proxy.exe in DualDesk 20 allows Remote Denial Of Service (daemon crash) via a long string to TCP port 5500. **CVE ID : CVE-2018-7583**	https://www.exploit-db.com/exploits/44222/	A-ADV-DUALD-20418/2
Afian					
Filerun					
Sql	06-03-2018	6.5	Afian FileRun (before 2018.02.13) suffers from a remote SQL injection vulnerability, when logged in as superuser, via the search parameter in a /?module=metadata&section=cpanel&page=list_filetypes request. **CVE ID : CVE-2018-7735**	NA	A-AFI-FILER-20418/3
Filerun					
Sql	06-03-2018	6.5	Afian FileRun (before 2018.02.13) suffers from a remote SQL injection vulnerability, when logged in as superuser, via the search parameter in a /?module=users&section=cpanel&page=list request. **CVE ID : CVE-2018-7734**	NA	A-AFI-FILER-20418/4
Amazon					
Amazon Music					
Exec Code	01-03-2018	6.8	This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Amazon Music Player 6.1.5.1213. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw	NA	A-AMA-AMAZO-20418/5

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			exists within the processing of URI handlers. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code under the context of the current process. Was ZDI-CAN-5521. **CVE ID : CVE-2018-1169**		
Antsle					
Antman					
Bypass	06-03-2018	7.5	antsle antman before 0.9.1a allows remote attackers to bypass authentication via invalid characters in the username and password parameters, as demonstrated by a username=>&password=%0a string to the /login URI. This allows obtaining root permissions within the web management console, because the login process uses Java's ProcessBuilder class and a bash script called antsle-auth with insufficient input validation. **CVE ID : CVE-2018-7739**	NA	A-ANT-ANTMA-20418/6
Apache					
ODE					
Directory Traversal	05-03-2018	6.4	The ODE process deployment web service was sensible to deployment messages with forged names. Using a path for the name was allowing directory traversal, resulting in the potential writing of files under unwanted locations, the overwriting of existing files or their deletion. This issue was addressed in Apache ODE 1.3.3 which was released in 2009, however the incorrect name CVE-2008-2370 was used on the advisory by mistake. **CVE ID : CVE-2018-1316**	NA	A-APA-ODE-20418/7
Xerces-c++					
NA	01-03-2018	7.5	In Apache Xerces-C XML Parser library before 3.2.1, processing of external DTD paths can result in a null pointer dereference under certain conditions. **CVE ID : CVE-2017-12627**	http://xerces.apache.org/xerces-c/secadv/CVE-2017-	A-APA-XERCE-20418/8

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
				12627.txt	
Apache;Redhat					
Activemq Artemis/Hornetq;Jboss Enterprise Application Platform					
NA	07-03-2018	7.8	It was found that when Artemis and HornetQ before 2.4.0 are configured with UDP discovery and JGroups discovery a huge byte array is created when receiving an unexpected multicast message. This may result in a heap memory exhaustion, full GC, or OutOfMemoryError. **CVE ID : CVE-2017-12174**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12174	A-APA-ACTIV-20418/9
Arubanetworks					
Web Management Portal					
Execute Code	09-03-2018	7.5	Unrestricted file upload vulnerability in Aruba Web Management portal allows remote attackers to execute arbitrary code by uploading a file with an executable extension. **CVE ID : CVE-2014-2592**	https://www.portcullis-security.com/security-research-and-downloads/security-advisories/CVE-2014-2592/	A-ARU-WEB M-20418/10
Atom					
Electron					
Execute Code Bypass	07-03-2018	9.3	Github Electron version Electron 1.8.2-beta.4 and earlier contains a Command Injection vulnerability in Protocol Handler that can result in command execute. This attack appear to be exploitable via the victim opening an electron protocol handler in their browser. This vulnerability appears to have been fixed in Electron 1.8.2-beta.5. This issue is due to an incomplete fix for CVE ID : CVE-2018-1000006, specifically the black list used was not case insensitive allowing an attacker to potentially bypass it. **CVE ID : CVE-2018-1000118**	https://electronjs.org/releases#1.8.2-beta.5	A-ATO-ELECT-20418/11
Aws-lambda-multipart-parser Project					

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Aws-lambda-multipart-parser					
DoS	04-03-2018	5	index.js in the Anton Myshenin aws-lambda-multipart-parser NPM package before 0.1.2 has a Regular Expression Denial of Service (ReDoS) issue via a crafted multipart/form-data boundary string. **CVE ID : CVE-2018-7560**	https://github.com/myshenin/aws-lambda-multipart-parser/commit/56ccb03af4dddebc2b2defb348b6558783d5757e	A-AWS-AWS-L-20418/12
3CX					
3CX					
Directory Traversal	03-03-2018	4	On 3CX 15.5.6354.2 devices, the parameter "file" in the request "/api/RecordingList/download?file=" allows full access to files on the server via path traversal. **CVE ID : CVE-2018-7654**	NA	A-3CX-3CX-20418/13
Bacula-web					
Bacula-web					
Sql	07-03-2018	7.5	Bacula-web before 8.0.0-rc2 is affected by multiple SQL Injection vulnerabilities that could allow an attacker to access the Bacula database and, depending on configuration, escalate privileges on the server. **CVE ID : CVE-2017-15367**	http://bacula-web.org/download/articles/bacula-web-8-0-0-rc2.html	A-BAC-BACUL-20418/14
Cactusvpn					
Cactusvpn					
Execute Code	05-03-2018	10	CactusVPN through 6.0 for macOS suffers from a root privilege escalation vulnerability in its privileged helper tool. The privileged helper tool implements an XPC interface, which allows arbitrary applications to execute system commands as root. **CVE ID : CVE-2018-7493**	https://github.com/VerSprite/research/blob/master/advisories/VS-2018-007.md	A-CAC-CACTU-20418/15
Calibre-ebook					
Calibre					
Execute Code	08-03-2018	6.8	gui2/viewer/bookmarkmanager.py in	https://bug	A-CAL-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			Calibre 3.18 calls cPickle.load on imported bookmark data, which allows remote attackers to execute arbitrary code via a crafted .pickle file, as demonstrated by Python code that contains an os.system call. **CVE ID : CVE-2018-7889**	s.launchpad.net/calibre/+bug/1753870	CALIB-20418/16
Cimg					
Cimg					
NA	01-03-2018	6.8	An issue was discovered in CImg v.220. A double free in load_bmp in CImg.h occurs when loading a crafted bmp image. **CVE ID : CVE-2018-7589**	NA	A-CIM-CIMG-20418/17
Overflow	01-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image. **CVE ID : CVE-2018-7588**	NA	A-CIM-CIMG-20418/18
Overflow	01-03-2018	6.8	An issue was discovered in CImg v.220. DoS occurs when loading a crafted bmp image that triggers an allocation failure in load_bmp in CImg.h. **CVE ID : CVE-2018-7587**	https://github.com/xiaoqx/pocs/tree/master/cimg	A-CIM-CIMG-20418/19
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE ID : CVE-2018-7588. This is in a "32 bits colors" case, aka case 32. **CVE ID : CVE-2018-7641**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-20418/20
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE ID : CVE-2018-7588. This is in a Monochrome case, aka case 1. **CVE ID : CVE-2018-7640**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-20418/21
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "16 bits colors" case, aka case 16. **CVE ID : CVE-2018-7639**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-20418/22

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "256 colors" case, aka case 8.**CVE ID : CVE-2018-7638**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-20418/23
Overflow	02-03-2018	6.8	An issue was discovered in CImg v.220. A heap-based buffer over-read in load_bmp in CImg.h occurs when loading a crafted bmp image, a different vulnerability than CVE-2018-7588. This is in a "16 colors" case, aka case 4.**CVE ID : CVE-2018-7637**	https://github.com/dtschump/CImg/issues/185	A-CIM-CIMG-20418/24
Cisco					
Data Center Network Manager					
Cross-Site Request Forgery	08-03-2018	6.8	A vulnerability in the web-based management interface of Cisco Data Center Network Manager could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections on the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on a targeted device via a web browser and with the privileges of the user. Cisco Bug IDs: CSCvg88291. **CVE ID : CVE-2018-0210**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-dcnm	A-CIS-DATA -20418/25
Email Encryption					
Execute Code XSS	08-03-2018	3.5	A vulnerability in the web-based management interface of the (cloud based) Cisco Registered Envelope Service could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected service. The vulnerability is due to insufficient validation of user-supplied	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-res	A-CIS-EMAIL-20418/26

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			input that is processed by the web-based management interface of the affected service. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information. Cisco Bug IDs: CSCvg74126. **CVE ID : CVE-2018-0208**		
Identity Services Engine					
Execute Code XSS	08-03-2018	4.3	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) 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. 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. Cisco Bug IDs: CSCvf69963. **CVE ID : CVE-2018-0212**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise1	A-CIS-IDENT-20418/27
Execute Code	08-03-2018	4.6	A vulnerability in certain CLI commands of Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to execute arbitrary commands on the host operating system with the privileges of the local user, aka Command Injection. These commands should have been restricted from this user. The vulnerability is due to insufficient input validation of CLI command user input. An attacker could exploit this vulnerability by authenticating to the targeted device	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise3	A-CIS-IDENT-20418/28

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			and issuing a CLI command with crafted user input. A successful exploit could allow the attacker to execute arbitrary commands on the affected system that should be restricted. The attacker would need to have valid user credentials for the device. Cisco Bug IDs: CSCvf49844. **CVE ID : CVE-2018-0214**		
DoS	08-03-2018	4.9	A vulnerability in specific CLI commands for the Cisco Identity Services Engine could allow an authenticated, local attacker to cause a denial of service (DoS) condition. The device may need to be manually rebooted to recover. The vulnerability is due to lack of proper input validation of the CLI user input for certain CLI commands. An attacker could exploit this vulnerability by authenticating to the device and issuing a crafted, malicious CLI command on the targeted device. A successful exploit could allow the attacker to cause a DoS condition. The attacker must have valid administrative privileges on the device to exploit this vulnerability. Cisco Bug IDs: CSCvf63414, CSCvh51992. **CVE ID : CVE-2018-0211**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise	A-CIS-IDENT-20418/29
Cross-Site Request Forgery	08-03-2018	5.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on a targeted device via a web browser and with the privileges of the user. Cisco Bug	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise5	A-CIS-IDENT-20418/30

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			IDs: CSCvf69805. **CVE ID : CVE-2018-0216**		
Gain Privileges	08-03-2018	6.5	A vulnerability in the credential reset functionality for Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to gain elevated privileges. The vulnerability is due to a lack of proper input validation. An attacker could exploit this vulnerability by authenticating to the device and sending a crafted HTTP request. A successful exploit could allow the attacker to gain elevated privileges to access functionality that should be restricted. The attacker must have valid user credentials to the device to exploit this vulnerability. Cisco Bug IDs: CSCvf69753. **CVE ID : CVE-2018-0213**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise2	A-CIS-IDENT-20418/31
Cross-Site Request Forgery	08-03-2018	6.8	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. The vulnerability is due to insufficient CSRF protections on the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on a targeted device via a web browser and with the privileges of the user. Cisco Bug IDs: CSCuv32863. **CVE ID : CVE-2018-0215**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-ise4	A-CIS-IDENT-20418/32
NA	08-03-2018	7.2	A vulnerability in specific CLI commands for the Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to perform command injection to the underlying operating system or cause a hang or disconnect of the user	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/c	A-CIS-IDENT-20418/33

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			session. The attacker needs valid administrator credentials for the device. The vulnerability is due to incomplete input validation of user input for certain CLI ISE configuration commands. An attacker could exploit this vulnerability by authenticating as an administrative user, issuing a specific CLI command, and entering crafted, malicious user input for the command parameters. An exploit could allow the attacker to perform command injection to the lower-level Linux operating system. It is also possible the attacker could cause the ISE user interface for this management session to hang or disconnect. Cisco Bug IDs: CSCvg95479. **CVE ID : CVE-2018-0221**	isco-sa-20180307-ise6	
Prime Collaboration;Prime Collaboration Assurance;Prime Collaboration Provisioning					
Gain Privileges	08-03-2018	7.2	A vulnerability in Cisco Prime Collaboration Provisioning (PCP) Software 11.6 could allow an unauthenticated, local attacker to log in to the underlying Linux operating system. The vulnerability is due to a hard-coded account password on the system. An attacker could exploit this vulnerability by connecting to the affected system via Secure Shell (SSH) using the hard-coded credentials. A successful exploit could allow the attacker to access the underlying operating system as a low-privileged user. After low-level privileges are gained, the attacker could elevate to root privileges and take full control of the device. Cisco Bug IDs: CSCvc82982. **CVE ID : CVE-2018-0141**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-cpcp	A-CIS-PRIME-20418/34
Prime Data Center Network Manager					
Execute Code XSS	08-03-2018	4.3	A vulnerability in the web-based management interface of Cisco Prime Data Center Network Manager could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/c	A-CIS-PRIME-20418/35

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			based management interface of an affected device. 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. Cisco Bug IDs: CSCvg81051. **CVE ID : CVE-2018-0144**	isco-sa-20180307-pdcnm	
Secure Access Control Server Solution Engine					
Gain Information	08-03-2018	4.3	A vulnerability in the web-based user interface of the Cisco Secure Access Control Server prior to 5.8 patch 9 could allow an unauthenticated, remote attacker to gain read access to certain information in the affected system. The vulnerability is due to improper handling of XML External Entities (XXEs) when parsing an XML file. An attacker could exploit this vulnerability by convincing the administrator of an affected system to import a crafted XML file. Cisco Bug IDs: CVE70616. **CVE ID : CVE-2018-0218**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs1	A-CIS-SECUR-20418/36
Gain Information	08-03-2018	4.3	A vulnerability in the web-based user interface of the Cisco Secure Access Control Server prior to 5.8 patch 9 could allow an unauthenticated, remote attacker to gain read access to certain information in the affected system. The vulnerability is due to improper handling of XML External Entities (XXEs) when parsing an XML file. An attacker could exploit this vulnerability by convincing the administrator of an affected system to import a crafted XML file. Cisco Bug IDs: CVE70595. **CVE ID : CVE-2018-0207**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs	A-CIS-SECUR-20418/37

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Secure Access Control System					
Execute Code	08-03-2018	10	A vulnerability in Java deserialization used by Cisco Secure Access Control System (ACS) prior to release 5.8 patch 9 could allow an unauthenticated, remote attacker to execute arbitrary commands on an affected device. The vulnerability is due to insecure deserialization of user-supplied content by the affected software. An attacker could exploit this vulnerability by sending a crafted serialized Java object. An exploit could allow the attacker to execute arbitrary commands on the device with root privileges. Cisco Bug IDs: CSCvh25988. **CVE ID : CVE-2018-0147**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs2	A-CIS-SECUR-20418/38
Security Manager					
Execute Code XSS	08-03-2018	4.3	A vulnerability in DesktopServlet in the web-based management interface of Cisco Security Manager could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based interface. 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. Cisco Bug IDs: CSCuy79668. **CVE ID : CVE-2018-0223**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-sm	A-CIS-SECUR-20418/39
Unified Computing System Director					
Execute Code XSS	08-03-2018	4.3	A vulnerability in the web-based management interface of Cisco Unified Computing System (UCS) Director could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/c	A-CIS-UNIFI-20418/40

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			based management interface of an affected device. 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. Cisco Bug IDs: CSCvg86518. **CVE ID : CVE-2018-0219**	isco-sa-20180307-ucs	
Videoscape Anyres Live					
Execute Code XSS	08-03-2018	3.5	A vulnerability in the web-based management interface of Cisco Videoscape AnyRes Live could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. 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. Cisco Bug IDs: CSCvg87525. **CVE ID : CVE-2018-0220**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-val	A-CIS-VIDEO-20418/41
Citrix					
Netscaler Application Delivery Controller;Netscaler Gateway;Netscaler Sd-wan					
Execute Code	01-03-2018	5	Command injection vulnerability in Citrix NetScaler ADC and NetScaler Gateway 11.0 before build 70.16, 11.1 before build 55.13, and 12.0 before build 53.13; and the NetScaler Load Balancing instance distributed with NetScaler SD-	https://support.citrix.com/article/CTX232199	A-CIT-NETSC-20418/42

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			WAN/CloudBridge 4000, 4100, 5000 and 5100 WAN Optimization Edition 9.3.0 allows remote attackers to execute a system command or read arbitrary files via an SSH login prompt. **CVE ID : CVE-2018-5314**		
Clip-bucket					
Clipbucket					
Sql	05-03-2018	7.5	An issue was discovered in ClipBucket before 4.0.0 Release 4902. SQL injection vulnerabilities exist in the actions/vote_channel.php channelId parameter, the ajax/commonAjax.php email parameter, and the ajax/commonAjax.php username parameter. **CVE ID : CVE-2018-7666**	NA	A-CLI-CLIPB-20418/43
NA	05-03-2018	10	An issue was discovered in ClipBucket before 4.0.0 Release 4902. A malicious file can be uploaded via the name parameter to actions/beats_uploader.php or actions/photo_uploader.php, or the coverPhoto parameter to edit_account.php. **CVE ID : CVE-2018-7665**	NA	A-CLI-CLIPB-20418/44
NA	05-03-2018	10	An issue was discovered in ClipBucket before 4.0.0 Release 4902. Any OS commands can be injected via shell metacharacters in the file_name parameter to /api/file_uploader.php or /actions/file_downloader.php. **CVE ID : CVE-2018-7664**	NA	A-CLI-CLIPB-20418/45
Cmsmadesimple					
Cms Made Simple					
XSS	11-03-2018	3.5	CMS Made Simple (CMSMS) 2.2.6 has XSS in admin/moduleinterface.php via the pagedata parameter. **CVE ID : CVE-2018-8058**	https://github.com/ibey0nd/CVE ID : CVE/blob/master/CMS%20Made%20Simple%20Stored%20XSS%202.md	A-CMS-CMS M-20418/46

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
XSS	11-03-2018	3.5	CMS Made Simple (CMSMS) 2.2.6 has stored XSS in admin/moduleinterface.php via the metadata parameter. **CVE ID : CVE-2018-7893**	https://github.com/ibey0nd/CVE ID : CVE/blob/master/CMS%20Made%20Simple%20Stored%20XSS.md	A-CMS-CMS M-20418/47
Couchcms					
Couch					
Gain Information	04-03-2018	5	Couch through 2.0 allows remote attackers to discover the full path via a direct request to includes/mysql2i/mysql2i.func.php or addons/phpmailer/phpmailer.php. **CVE ID : CVE-2018-7662**	https://github.com/CouchCMS/CouchCMS/issues/46	A-COU-COUCH-20418/48
Dell					
Emc Vmax Embedded Management					
NA	08-03-2018	9	An arbitrary file upload vulnerability was discovered in vApp Manager which is embedded in Dell EMC Unisphere for VMAX, Dell EMC Solutions Enabler, Dell EMC VASA Virtual Appliances, and Dell EMC VMAX Embedded Management (eManagement): Dell EMC Unisphere for VMAX Virtual Appliance versions prior to 8.4.0.18, Dell EMC Solutions Enabler Virtual Appliance versions prior to 8.4.0.21, Dell EMC VASA Virtual Appliance versions prior to 8.4.0.514, and Dell EMC VMAX Embedded Management (eManagement) versions prior to and including 1.4 (Enginuity Release 5977.1125.1125 and earlier). A remote authenticated malicious user may potentially upload arbitrary maliciously crafted files in any location on the web server. By chaining this vulnerability with CVE ID : CVE-2018-1216, the attacker may use the default account to exploit this vulnerability.	http://seclists.org/fulldisclosure/2018/Feb/41	A-DEL-EMC V-20418/49

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-1215		
NA	08-03-2018	10	A hard-coded password vulnerability was discovered in vApp Manager which is embedded in Dell EMC Unisphere for VMAX, Dell EMC Solutions Enabler, Dell EMC VASA Virtual Appliances, and Dell EMC VMAX Embedded Management (eManagement): Dell EMC Unisphere for VMAX Virtual Appliance versions prior to 8.4.0.18, Dell EMC Solutions Enabler Virtual Appliance versions prior to 8.4.0.21, Dell EMC VASA Virtual Appliance versions prior to 8.4.0.514, and Dell EMC VMAX Embedded Management (eManagement) versions prior to and including 1.4 (Enginuity Release 5977.1125.1125 and earlier). They contain an undocumented default account (smc) with a hard-coded password that may be used with certain web servlets. A remote attacker with the knowledge of the hard-coded password and the message format may use vulnerable servlets to gain unauthorized access to the system. Note: This account cannot be used to log in via the web user interface. **CVE ID : CVE-2018-1216**	http://seclists.org/fulldisclosure/2018/Feb/41	A-DEL-EMC V-20418/50
D-link					
Mydlink+					
NA	05-03-2018	4.3	An issue was discovered in D-Link mydlink+ 3.8.5 build 259 for DCS-933L 1.05.04 and DCS-934L 1.05.04 devices. The mydlink+ app sends the username and password for connected D-Link cameras (such as DCS-933L and DCS-934L) unencrypted from the app to the camera, allowing attackers to obtain these credentials and gain control of the camera including the ability to view the camera's stream and make changes without the user's knowledge. **CVE ID : CVE-2018-7698**	http://www.nettexsolutions.com/2018/03/04/d-link-security-cameras-using-mydlink-leak-passwords-to-the-internet/	A-D-L-MYDLI-20418/51
EMC					

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
Rsa Identity Governance And Lifecycle;Rsa Identity Management And Governance;Rsa Via Lifecycle And Governance					
NA	08-03-2018	7.2	An issue was discovered in EMC RSA Identity Governance and Lifecycle versions 7.0.1, 7.0.2, all patch levels (hardware appliance and software bundle deployments only); RSA Via Lifecycle and Governance version 7.0, all patch levels (hardware appliance and software bundle deployments only); RSA Identity Management & Governance (RSA IMG) versions 6.9.0, 6.9.1, all patch levels (hardware appliance and software bundle deployments only). It allows certain OS level users to execute arbitrary scripts with root level privileges. **CVE ID : CVE-2018-1182**	http://seclists.org/fulldisclosure/2018/Mar/16	A-EMC-RSA I-20418/52
Enalean					
Tuleap					
Cross-Site Request Forgery	01-03-2018	6.8	An issue was discovered in Enalean Tuleap 9.17. Lack of CSRF attack mitigation while changing an e-mail address makes it possible to abuse the functionality by attackers. By making a CSRF attack, an attacker could make a victim change his registered e-mail address on the application, leading to account takeover. **CVE ID : CVE-2018-7634**	https://github.com/Enalean/tuleap/commit/0843c046eee54b16ec6a7753c575838212770189	A-ENA-TULEA-20418/53
Eramba					
Eramba					
XSS	07-03-2018	4.3	Eramba e1.0.6.033 has Reflected XSS in the Date Filter via the created parameter to the /crons URI. **CVE ID : CVE-2018-7741**	https://medium.com/stolabs/security-issues-on-eramba-cf887bc0a069	A-ERA-ERAMB-20418/54
XSS File Inclusion	09-03-2018	4.3	Eramba e1.0.6.033 has Reflected XSS on the Error page of the CSV file inclusion tab of the /importTool/preview URI, with a CSV file polluted with malicious JavaScript.	https://medium.com/stolabs/security-issues-on-eramba-	A-ERA-ERAMB-20418/55

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-7997	cf887bc0a069	
XSS	09-03-2018	4.3	Eramba e1.0.6.033 has Stored XSS on the tooltip box via the /programScopes description parameter. **CVE ID : CVE-2018-7996**	https://medium.com/stolabs/security-issues-on-eramba-cf887bc0a069	A-ERA-ERAMB-20418/56
XSS	09-03-2018	4.3	Eramba e1.0.6.033 has Reflected XSS in reviews/filterIndex/ThirdPartyRiskReview via the advanced_filter parameter (aka the Search Parameter). **CVE ID : CVE-2018-7894**	https://medium.com/stolabs/security-issues-on-eramba-cf887bc0a069	A-ERA-ERAMB-20418/57
Exempi Project					
Exempi					
NA	06-03-2018	4.3	An issue was discovered in Exempi through 2.4.4. XMPFiles/source/FormatSupport/WEBP_Support.cpp does not check whether a bitstream has a NULL value, leading to a NULL pointer dereference in the WEBP::VP8XChunk class. **CVE ID : CVE-2018-7731**	NA	A-EXE-EXEMP-20418/58
NA	06-03-2018	4.3	An issue was discovered in Exempi through 2.4.4. A certain case of a 0xffffffff length is mishandled in XMPFiles/source/FormatSupport/PSIR_FileWriter.cpp, leading to a heap-based buffer over-read in the PSD_MetaHandler::CacheFileData() function. **CVE ID : CVE-2018-7730**	NA	A-EXE-EXEMP-20418/59
NA	06-03-2018	4.3	An issue was discovered in Exempi through 2.4.4. There is a stack-based buffer over-read in the PostScript_MetaHandler::ParsePSFile() function in XMPFiles/source/FileHandlers/PostScript_Handler.cpp. **CVE ID : CVE-2018-7729**	NA	A-EXE-EXEMP-20418/60
NA	06-03-2018	4.3	An issue was discovered in Exempi	NA	A-EXE-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			through 2.4.4. XMPFiles/source/FileHandlers/TIFF_Handler.cpp mishandles a case of a zero length, leading to a heap-based buffer over-read in the MD5Update() function in third-party/zuid/interfaces/MD5.cpp. **CVE ID : CVE-2018-7728**		EXEMP-20418/61
Exponentcms					
Exponent Cms					
NA	03-03-2018	6.5	In Exponent CMS before 2.4.1 Patch #6, certain admin users can elevate their privileges. **CVE ID : CVE-2017-18213**	NA	A-EXP-EXPON-20418/62
NA	06-03-2018	7.5	Exponent CMS 2.3.0 through 2.3.9 allows remote attackers to have unspecified impact via vectors related to "uploading files to wrong location." **CVE ID : CVE-2016-7443**	http://www.exponentcms.org/news/patch-1-released-for-v2-3-9	A-EXP-EXPON-20418/63
F5					
Big-ip Access Policy Manager;Big-ip Advanced Firewall Manager;Big-ip Analytics;Big-ip Application Acceleration Manager;Big-ip Application Security Manager;Big-ip Dns;Big-ip Edge Gateway;Big-ip Global Traffic Manager;Big-ip Link Controller;Big-ip Local Traffic Manager;Big-ip Policy Enforcement Manager;Big-ip Webaccelerator;Big-ip Websafe					
NA	01-03-2018	4.3	In some circumstances, on F5 BIG-IP systems running 13.0.0, 12.1.0 - 12.1.3.1, any 11.6.x or 11.5.x release, or 11.2.1, TCP DNS profile allows excessive buffering due to lack of flow control. **CVE ID : CVE-2018-5501**	https://support.f5.com/csp/article/K44200194	A-F5-BIG-I-20418/64
NA	01-03-2018	4.3	On F5 BIG-IP systems running 13.0.0, 12.1.0 - 12.1.3.1, or 11.6.1 - 11.6.2, every Multipath TCP (MCTCP) connection established leaks a small amount of memory. Virtual server using TCP profile with Multipath TCP (MCTCP) feature enabled will be affected by this issue. **CVE ID : CVE-2018-5500**	https://support.f5.com/csp/article/K33211839	A-F5-BIG-I-20418/65
NA	01-03-2018	7.8	Under certain conditions for F5 BIG-IP systems 13.0.0 or 12.1.0 - 12.1.3.1, using FastL4 profiles, when the Reassemble IP Fragments option is disabled (default), some specific large fragmented packets may restart the Traffic Management	https://support.f5.com/csp/article/K62712037	A-F5-BIG-I-20418/66

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			Microkernel (TMM). **CVE ID : CVE-2017-6150**		
Big-ip Application Security Manager					
NA	01-03-2018	5	On F5 BIG-IP systems running 13.0.0, 12.1.0 - 12.1.3.1, or 11.6.1 - 11.6.2, the BIG-IP ASM bd daemon may core dump memory under some circumstances when processing undisclosed types of data on systems with 48 or more CPU cores. **CVE ID : CVE-2017-6154**	https://support.f5.com/csp/article/K38243073	A-F5-BIG-I-20418/67
Ftpshell					
Ftpshell Client					
Overflow	01-03-2018	10	An issue was discovered in FTPShell Client 6.7. A remote FTP server can send 400 characters of 'F' in conjunction with the FTP 220 response code to crash the application; after this overflow, one can run arbitrary code on the victim machine. This is similar to CVE-2009-3364 and CVE-2017-6465. **CVE ID : CVE-2018-7573**	https://cxsecurity.com/issue/WLB-2018030011	A-FTP-FTPSH-20418/68
Gemalto					
Safenet Authentication Service End User Software Tools For Windows					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service End User Software Tools for Windows uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7596**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/69
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service for AD FS Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7963**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/70
Safenet Authentication Service For Citrix Web Interface Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service for Citrix Web Interface Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an	https://safenet.gemalto.com/technical-support/sec	A-GEM-SAFEN-20418/71

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			executable module. **CVE ID : CVE-2015-7967**	urity-updates/	
Safenet Authentication Service For Nps Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service for NPS Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7964**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/72
Safenet Authentication Service For Outlook Web App Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service for Outlook Web App Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7962**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/73
Safenet Authentication Service Iis Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service IIS Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7597**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/74
Safenet Authentication Service Remote Web Workplace Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service Remote Web Workplace Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7961**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/75
Safenet Authentication Service Tokenvalidator Proxy Agent					
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service TokenValidator Proxy Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module. **CVE ID : CVE-2015-7598**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/76
Safenet Authentication Service Windows Logon Agent					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service Windows Logon Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module, a different vulnerability than CVE ID : CVE-2015-7965. **CVE ID : CVE-2015-7966**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/77
Gain Privileges	02-03-2018	4.6	SafeNet Authentication Service Windows Logon Agent uses a weak ACL for unspecified installation directories and executable modules, which allows local users to gain privileges by modifying an executable module, a different vulnerability than CVE-2015-7966. **CVE ID : CVE-2015-7965**	https://safenet.gemalto.com/technical-support/security-updates/	A-GEM-SAFEN-20418/78
Giribaz					
File Manager					
NA	07-03-2018	5	inc/logger.php in the Giribaz File Manager plugin before 5.0.2 for WordPress logged activity related to the plugin in /wp-content/uploads/file-manager/log.txt. If a user edits the wp-config.php file using this plugin, the wp-config.php contents get added to log.txt, which is not protected and contains database credentials, salts, etc. These files have been indexed by Google and a simple dork will find affected sites. **CVE ID : CVE-2018-7204**	https://wordpress.org/plugins/file-manager/#developers	A-GIR-FILE -20418/79
GNU					
Binutils					
DoS	02-03-2018	4.3	The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy. **CVE ID : CVE-2018-7642**	NA	A-GNU-BINUT-20418/80

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
DoS Overflow	02-03-2018	6.8	The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump. **CVE ID : CVE-2018-7643**	NA	A-GNU-BINUT-20418/81
Gpac Project					
Gpac					
Overflow	06-03-2018	6.8	GPAC MP4Box version 0.7.1 and earlier contains a Buffer Overflow vulnerability in src/isomedia/avc_ext.c lines 2417 to 2420 that can result in Heap chunks being modified, this could lead to RCE. This attack appear to be exploitable via an attacker supplied MP4 file that when run by the victim may result in RCE. **CVE ID : CVE-2018-1000100**	https://github.com/gpac/gpac/issues/994	A-GPA-GPAC-20418/82
Overflow	07-03-2018	6.8	GPAC through 0.7.1 has a Buffer Overflow in the gf_media_avc_read_sps function in media_tools/av_parsers.c, a different vulnerability than CVE-2018-1000100. **CVE ID : CVE-2018-7752**	https://github.com/gpac/gpac/commit/90dc7f853d31b0a4e9441cba97feccf36d8b69a4	A-GPA-GPAC-20418/83
Graphicsmagick					
Graphicsmagick					
DoS	05-03-2018	4.3	An issue was discovered in GraphicsMagick 1.3.26. An allocation failure vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted file that triggers an attempt at a large png_pixels array allocation. **CVE ID : CVE-2017-18219**	https://sourceforge.net/p/graphicsmagick/bugs/459/	A-GRA-GRAPH-20418/84
DoS	13-03-2018	4.3	An issue was discovered in GraphicsMagick 1.3.26. A NULL pointer dereference vulnerability was found in the function ReadEnhMetaFile in coders/emf.c, which allows attackers to	https://sourceforge.net/p/graphicsmagick/bugs/475/	A-GRA-GRAPH-20418/85

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			cause a denial of service via a crafted file. **CVE ID : CVE-2017-18231**		
DoS	13-03-2018	4.3	An issue was discovered in GraphicsMagick 1.3.26. A NULL pointer dereference vulnerability was found in the function ReadCINEONImage in coders/cineon.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2017-18230**	https://sourceforge.net/p/graphicsmagick/bugs/473/	A-GRA-GRAPH-20418/86
DoS	05-03-2018	6.8	The ReadOneJNGImage and ReadJNGImage functions in coders/png.c in GraphicsMagick 1.3.26 allow remote attackers to cause a denial of service (magick/blob.c CloseBlob use-after-free) or possibly have unspecified other impact via a crafted file, a related issue to CVE-2017-11403. **CVE ID : CVE-2017-18220**	https://sourceforge.net/p/graphicsmagick/bugs/438/	A-GRA-GRAPH-20418/87
Hoosk					
Hoosk					
Cross-Site Request Forgery	01-03-2018	6.8	CSRF exists in Hoosk 1.7.0 via /admin/users/new/add, resulting in account creation. **CVE ID : CVE-2018-7590**	https://github.com/havok89/Hoosk/issues/45	A-HOO-HOOSK-20418/88
Hot Scripts Clone Project					
Hot Scripts Clone					
XSS	06-03-2018	3.5	PHP Scripts Mall Hot Scripts Clone:Script Classified Version 3.1 Application is vulnerable to stored XSS within the "Add New" function for a Management User. Within the "Add New" section, the application does not sanitize user supplied input to the name parameter, and renders injected JavaScript code to the user's browser. This is different from CVE-2018-6878. **CVE ID : CVE-2018-7650**	https://neetech18.blogspot.in/2018/03/stored-xss-vulnerability-in-hot-scripts.html	A-HOT-HOT S-20418/89
HP					
Operations Orchestration					
DoS	01-03-2018	7.8	Denial of Service vulnerability in Micro Focus Operations Orchestration Software, version 10.x. This vulnerability could be remotely exploited to allow Denial of Service.	https://softwaresupport.softwaregrp.com/document/-	A-HP-OPERA-20418/90

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-6490	/facetsearch/document/KM03103896	
HTC;Volkswagen					
Customer-link Bridge/Customer-link					
NA	01-03-2018	8.3	This vulnerability allows adjacent attackers to inject arbitrary Controller Area Network messages on vulnerable installations of Volkswagen Customer-Link App 1.30 and HTC Customer-Link Bridge. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Customer-Link App and Customer-Link Bridge. The issue results from the lack of a proper protection mechanism against unauthorized firmware updates. An attacker can leverage this vulnerability to inject CAN messages. Was ZDI-CAN-5264. **CVE ID : CVE-2018-1170**	https://zerodayinitiative.com/advisories/ZDI-18-214	A-HTC-CUSTO-20418/91
IBM					
Application Performance Management;Cloud Apm Data Collector;Monitoring					
Gain Information	08-03-2018	5	IBM Application Performance Management for Monitoring & Diagnostics (IBM Monitoring 8.1.3 and 8.1.4) may release sensitive personal data to the staff who can access to the database of this product. IBM X-Force ID: 138210. **CVE ID : CVE-2018-1387**	http://www.ibm.com/support/docview.wss?uid=swg22014035	A-IBM-APPLI-20418/92
Financial Transaction Manager					
NA	09-03-2018	3.5	IBM Financial Transaction Manager (FTM) for ACH Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, Financial Transaction Manager (FTM) for Check Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, and Financial Transaction Manager (FTM) for Corporate Payment Services (CPS) for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013 allows remote attackers to conduct clickjacking attacks via a crafted web site. IBM X-Force ID:	http://www-01.ibm.com/support/docview.wss?uid=swg21977245	A-IBM-FINAN-20418/93

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			111076. **CVE ID : CVE-2016-0274**		
XSS	09-03-2018	3.5	Cross-site scripting (XSS) vulnerability in IBM Financial Transaction Manager (FTM) for ACH Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, Financial Transaction Manager (FTM) for Check Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, and Financial Transaction Manager (FTM) for Corporate Payment Services (CPS) for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. IBM X-Force ID: 110562. **CVE ID : CVE-2016-0253**	http://www-01.ibm.com/support/docview.wss?uid=swg21977245	A-IBM-FINAN-20418/94
Gain Information	09-03-2018	4	XML external entity (XXE) vulnerability in IBM Financial Transaction Manager (FTM) for ACH Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, Financial Transaction Manager (FTM) for Check Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, and Financial Transaction Manager (FTM) for Corporate Payment Services (CPS) for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013 allows remote authenticated users to obtain sensitive information via crafted XML data. IBM X-Force ID: 110915. **CVE ID : CVE-2016-0268**	http://www-01.ibm.com/support/docview.wss?uid=swg21977245	A-IBM-FINAN-20418/95
Cross-Site Request Forgery	09-03-2018	6	Cross-site request forgery (CSRF) vulnerability in IBM Financial Transaction Manager (FTM) for ACH Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, Financial Transaction Manager (FTM) for Check Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, and Financial Transaction Manager (FTM) for Corporate Payment Services (CPS) for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013 allows remote attackers to hijack the authentication of arbitrary users via	http://www-01.ibm.com/support/docview.wss?uid=swg21977245	A-IBM-FINAN-20418/96

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			unspecified vectors. IBM X-Force ID: 111052. **CVE ID : CVE-2016-0272**		
Execute Code	09-03-2018	6.5	IBM Financial Transaction Manager (FTM) for ACH Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, Financial Transaction Manager (FTM) for Check Services for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013, and Financial Transaction Manager (FTM) for Corporate Payment Services (CPS) for Multi-Platform 2.1.1.2 and 3.0.0.x before fp0013 allows remote attackers to execute arbitrary code via a crafted serialized Java Message Service (JMS) ObjectMessage object. IBM X-Force ID: 111084.**CVE ID : CVE-2016-0276**	http://www-01.ibm.com/support/docview.wss?uid=swg21977245	A-IBM-FINAN-20418/97
Monitoring					
Cross-Site Request Forgery	08-03-2018	6.8	IBM Application Performance Management - Response Time Monitoring Agent (IBM Monitoring 8.1.4) is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 139598. **CVE ID : CVE-2018-1442**	http://www.ibm.com/support/docview.wss?uid=swg22013500	A-IBM-MONIT-20418/98
Qradar Pulse					
Gain Information	08-03-2018	5	IBM Pulse for QRadar 1.0.0 - 1.0.3 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM X-Force ID: 133123. **CVE ID : CVE-2017-1625**	http://www.ibm.com/support/docview.wss?uid=swg22014284	A-IBM-QRADA-20418/99
Security Access Manager;Tivoli Federated Identity Manager					
NA	08-03-2018	4.6	An XML parsing vulnerability affects IBM SAML-based single sign-on (SSO) systems (IBM Security Access Manager 9.0.0 - 9.0.4 and IBM Tivoli Federated Identity Manager 6.2 - 6.0.2.) This vulnerability can allow an attacker with authenticated access to trick SAML systems into authenticating as a different user without knowledge of the victim users password.	http://www.ibm.com/support/docview.wss?uid=swg22014160	A-IBM-SECUR-20418/100

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			IBM X-Force ID: 139754. **CVE ID : CVE-2018-1443**		
Security Guardium Big Data Intelligence					
NA	02-03-2018	5	IBM Security Guardium Big Data Intelligence (SonarG) 3.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 137773. **CVE ID : CVE-2018-1373**	http://www.ibm.com/support/docview.wss?uid=swg22013750	A-IBM-SECUR-20418/101
Tivoli Business Service Manager					
Gain Information	09-03-2018	4	IBM Tivoli Business Service Manager 6.1.0 before 6.1.0-TIV-BSM-FP0004 and 6.1.1 before 6.1.1-TIV-BSM-FP0004 allows remote authenticated users to obtain administrator passwords by leveraging unspecified privileges. BM X-Force ID: 111234. **CVE ID : CVE-2016-0286**	http://www-01.ibm.com/support/docview.wss?uid=swg21986852	A-IBM-TIVOL-20418/102
Imagely					
Nextgen Gallery					
Directory Traversal	01-03-2018	5	In the nextgen-gallery plugin before 2.2.50 for WordPress, gallery paths are not secured. **CVE ID : CVE-2018-7586**	https://wordpress.org/plugins/nextgen-gallery/#developers	A-IMA-NEXTG-20418/103
Imagemagick					
Imagemagick					
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function WriteGIFImage in coders/gif.c, which allow remote attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2017-18254**	https://github.com/ImageMagick/ImageMagick/issues/808	A-IMA-IMAGE-20418/104
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LoadOpenCLDevices in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2017-18253**	https://github.com/ImageMagick/ImageMagick/issues/794	A-IMA-IMAGE-20418/105
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. The MogrifyImageList function in	https://github.com/Ima	A-IMA-IMAGE-

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			MagickWand/mogrify.c allows attackers to cause a denial of service (assertion failure and application exit in ReplaceImageInList) via a crafted file. **CVE ID : CVE-2017-18252**	geMagick/ImageMagick/issues/802	20418/ 106
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function ReadPCDImage in coders/pcd.c, which allow remote attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2017-18251**	https://github.com/ImageMagick/ImageMagick/issues/809	A-IMA-IMAGE-20418/ 107
DoS	26-03-2018	4.3	An issue was discovered in ImageMagick 7.0.7. A NULL pointer dereference vulnerability was found in the function LogOpenCLBuildFailure in MagickCore/opencl.c, which allows attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2017-18250**	https://github.com/ImageMagick/ImageMagick/issues/793	A-IMA-IMAGE-20418/ 108
NA	01-03-2018	6.8	In the GetOpenCLCachedFilesDirectory function in magick/opencl.c in ImageMagick 7.0.7, a NULL pointer dereference vulnerability occurs because a memory allocation result is not checked, related to Get Open CLCache Directory.**CVE ID : CVE-2017-18209**	NA	A-IMA-IMAGE-20418/ 109
NA	01-03-2018	7.5	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function saveBinaryCLProgram in magick/opencl.c because a program-lookup result is not checked, related to CacheOpenCLKernel. **CVE ID : CVE-2017-18211**	NA	A-IMA-IMAGE-20418/ 110
NA	01-03-2018	7.5	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function BenchmarkOpenCLDevices in MagickCore/opencl.c because a memory allocation result is not checked. **CVE ID : CVE-2017-18210**	NA	A-IMA-IMAGE-20418/ 111
Iobit					
Advanced Systemcare Ultimate					
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to	https://github.com/D0neMkj/POC_B	A-IOB-ADVAN-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE ID : CVE-2018-9007**	SOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060c4	112
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE ID : CVE-2018-9006**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c402004	A-IOB-ADVAN-20418/113
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE ID : CVE-2018-9005**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060d0	A-IOB-ADVAN-20418/114
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE ID : CVE-2018-9004**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060d0	A-IOB-ADVAN-20418/115
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to	https://github.com/D0neMkj/POC_B	A-IOB-ADVAN-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE ID : CVE-2018-9003**	SOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c402000	116
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE ID : CVE-2018-9002**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060cc	A-IOB-ADVAN-20418/117
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE ID : CVE-2018-9001**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c402000	A-IOB-ADVAN-20418/118
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE ID : CVE-2018-9000**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c402004	A-IOB-ADVAN-20418/119
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win7_x64.sys) allows local	https://github.com/D0neMkj/POC_B	A-IOB-ADVAN-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE ID : CVE-2018-8999**	SOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x64.sys-0x9c4060c4	120
DoS	24-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_x86.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE ID : CVE-2018-8998**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win7_x86.sys-0x9c4060cc	A-IOB-ADVAN-20418/121
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060cc. **CVE ID : CVE-2018-9044**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060cc	A-IOB-ADVAN-20418/122
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060d0. **CVE ID : CVE-2018-9043**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060d0	A-IOB-ADVAN-20418/123
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local	https://github.com/D0neMkj/POC_B	A-IOB-ADVAN-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402000. **CVE ID : CVE-2018-9042**	SOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c402000	124
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c402004. **CVE ID : CVE-2018-9041**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c402004	A-IOB-ADVAN-20418/125
DoS	26-03-2018	6.1	In Advanced SystemCare Ultimate 11.0.1.58, the driver file (Monitor_win10_x64.sys) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0x9c4060c4. **CVE ID : CVE-2018-9040**	https://github.com/D0neMkj/POC_BSOD/tree/master/Advanced%20SystemCare%20Utimate/Monitor_win10_x64.sys-0x9c4060c4	A-IOB-ADVAN-20418/126
Ithemes					
Security					
NA	02-03-2018	5	The iThemes Security plugin before 6.9.1 for WordPress does not properly perform data escaping for the logs page. **CVE ID : CVE-2018-7433**	https://wordpress.org/plugins/better-wp-security/#developers	A-ITH-SECUR-20418/127
Jasper Project					
Jasper					
DoS	27-03-2018	4.3	JasPer 2.0.14 allows denial of service via a reachable assertion in the function jpc_firstone in libjasper/jpc/jpc_math.c.	https://github.com/mdadams/jasper	A-JAS-JASPE-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-9055	/issues/172	128
Jease					
Jease					
XSS	07-03-2018	3.5	Cross-site scripting (XSS) vulnerability in Jease 2.11 allows remote authenticated users to inject arbitrary web script or HTML via a content section note. **CVE ID : CVE-2014-8780**	NA	A-JEA-JEASE-20418/129
Jerryscript					
Jerryscript					
Overflow	01-03-2018	7.5	An issue was discovered in JerryScript 1.0. There is a heap-based buffer over-read in the lit_read_code_unit_from_hex function in lit/lit-char-helpers.c via a RegExp("[\x0"); payload. **CVE ID : CVE-2017-18212**	https://github.com/jerryscript-project/jerryscript/issues/2140	A-JER-JERRY-20418/130
Jubat					
Jubatus					
Directory Traversal	09-03-2018	5	Directory traversal vulnerability in Jubatus 1.0.2 and earlier allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2018-0525**	NA	A-JUB-JUBAT-20418/131
Execute Code	09-03-2018	7.5	Jubatus 1.0.2 and earlier allows remote code execution via unspecified vectors. **CVE ID : CVE-2018-0524**	NA	A-JUB-JUBAT-20418/132
Metinfo					
Metinfo					
XSS	07-03-2018	4.3	Cross Site Scripting (XSS) exists in MetInfo 6.0.0 via /feedback/index.php because app/system/feedback/web/feedback.class.php mishandles input data. **CVE ID : CVE-2018-7721**	https://github.com/Gitaddy/vluns/blob/master/Metinfo.md	A-MET-METIN-20418/134
Mingw-w64					
Mingw-w64					
Overflow	06-03-2018	7.5	Mingw-w64 version 5.0.3 and earlier contains an Improper Null Termination (CWE-170) vulnerability in mingw-w64-crt (libc)->(v)snprintf that can result in The bug may be used to corrupt	NA	A-MIN-MINGW-20418/135

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			subsequent string functions. This attack appear to be exploitable via Depending on the usage, worst case: network. **CVE ID : CVE-2018-1000101**		
Moment Project					
Moment					
DoS	04-03-2018	5	The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a different vulnerability than CVE ID : CVE-2016-4055. **CVE ID : CVE-2017-18214**	https://nodesecurity.io/advisories/532	A-MOM-MOMEN-20418/136
Mozilla					
Bleach					
NA	07-03-2018	7.5	An issue was discovered in Bleach 2.1.x before 2.1.3. Attributes that have URI values weren't properly sanitized if the values contained character entities. Using character entities, it was possible to construct a URI value with a scheme that was not allowed that would slide through unsanitized. **CVE ID : CVE-2018-7753**	NA	A-MOZ-BLEAC-20418/137
Netiq					
Access Manager					
XSS	01-03-2018	4.3	A reflected cross site scripting attack in the NetIQ Access Manager before 4.3.3 using the "typecontainerid" parameter of the policy editor could allowed code injection into pages of authenticated users. **CVE ID : CVE-2017-14800**	https://www.novell.com/support/kb/doc.php?id=7022356	A-NET-ACCES-20418/138
XSS	01-03-2018	4.3	A cross site scripting attack in handling the ESP login parameter handling in NetIQ Access Manager before 4.3.3 could be used to inject javascript code into the login page. **CVE ID : CVE-2017-14799**	https://www.novell.com/support/kb/doc.php?id=7022358	A-NET-ACCES-20418/139
XSS	02-03-2018	4.3	Reflected XSS in the NetIQ Access Manager before 4.3.3 allowed attackers to reflect back xss into the called page using the url parameter. **CVE ID : CVE-2017-14801**	https://www.novell.com/support/kb/doc.php?id=7022357	A-NET-ACCES-20418/140
XSS	02-03-2018	4.3	Novell Access Manager iManager before	https://ww	A-NET-

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			4.3.3 did not validate parameters so that cross site scripting content could be reflected back into the result page using the "a" parameter. **CVE ID : CVE-2017-9276**	w.novell.com/support/kb/doc.php?id=7022359	ACCES-20418/141
NA	02-03-2018	5.8	Novell Access Manager Admin Console and IDP servers before 4.3.3 have a URL that could be used by remote attackers to trigger unvalidated redirects to third party sites. **CVE ID : CVE-2017-14802**	https://www.novell.com/support/kb/doc.php?id=7022360	A-NET-ACCES-20418/142
Cross-Site Request Forgery	14-03-2018	6.8	A CSRF exposure exists in NetIQ Access Manager (NAM) 4.4 Identity Server component. **CVE ID : CVE-2018-7677**	https://www.netiq.com/support/kb/doc.php?id=7022725	A-NET-ACCES-20418/143
Edirectory					
Execute Code	02-03-2018	6.5	The certificate upload in NetIQ eDirectory PKI plugin before 8.8.8 Patch 10 Hotfix 1 could be abused to upload JSP code which could be used by authenticated attackers to execute JSP applets on the iManager server. **CVE ID : CVE-2017-7429**	https://www.novell.com/support/kb/doc.php?id=3426981	A-NET-EDIRE-20418/144
NA	02-03-2018	7.5	NetIQ eDirectory before 9.0 SP4 did not enforce login restrictions when "ebaclient" was used, allowing unpermitted access to eDirectory services. **CVE ID : CVE-2017-9285**	https://www.novell.com/support/kb/doc.php?id=7016794	A-NET-EDIRE-20418/145
Imanager					
NA	02-03-2018	5	NetIQ iManager before 3.0.3 delivered a SSL private key in a Java application (JAR file) for authentication to Sentinel, allowing attackers to extract and establish their own connections to the Sentinel appliance. **CVE ID : CVE-2017-5189**	https://bugzilla.suse.com/show_bug.cgi?id=1021637	A-NET-IMANA-20418/146
Privileged Account Manager					
XSS	02-03-2018	4.3	NetIQ Privileged Account Manager before 3.1 Patch Update 3 allowed cross site scripting attacks via javascript DOM modification using the supplied cookie parameter. **CVE ID : CVE-2017-7438**	https://www.netiq.com/documentation/privileged-account-	A-NET-PRIVI-20418/147

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
				manager-3/npam3103-release-notes/data/npam3103-release-notes.html	
XSS	05-03-2018	4.3	NetIQ Privileged Account Manager before 3.1 Patch Update 3 allowed cross site scripting attacks via the "type" and "account" parameters of json requests. **CVE ID : CVE-2017-7437**	https://bugzilla.suse.com/show_bug.cgi?id=1001069	A-NET-PRIVI-20418/148
Sentinel					
Gain Information	07-03-2018	3.5	In NetIQ Sentinel before 8.1.x, a Sentinel user is logged into the Sentinel Web Interface. After performing some tasks within Sentinel the user does not log out but does go idle for a period of time. This in turn causes the interface to timeout so that it requires the user to re-authenticate. If another user is passing by and decides to login, their credentials are accepted. While The user does not inherit any of the other users privileges, they are able to view the previous screen. In this case it is possible that the user can see another users events or configuration information for whatever view is currently showing. **CVE ID : CVE-2018-7675**	https://www.netiq.com/support/kb/doc.php?id=7022706	A-NET-SENTI-20418/149
Novell					
Edirectory					
NA	02-03-2018	5	The LDAP backend in Novell eDirectory before 9.0 SP4 when switched to EBA (Enhanced Background Authentication) kept open connections without EBA. **CVE ID : CVE-2017-9277**	https://www.novell.com/support/kb/doc.php?id=7016794	A-NOV-EDIRE-20418/150
NA	02-03-2018	5	In Novell eDirectory before 9.0.3.1 the LDAP interface was not strictly enforcing cipher restrictions allowing weaker ciphers to be used during SSL BIND operations. **CVE ID : CVE-2017-9267**	https://www.novell.com/support/kb/doc.php?id=7016794	A-NOV-EDIRE-20418/151

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
NTP					
NTP					
NA	06-03-2018	4	ntpd in ntp 4.2.x before 4.2.8p7 and 4.3.x before 4.3.92 allows authenticated users that know the private symmetric key to create arbitrarily-many ephemeral associations in order to win the clock selection of ntpd and modify a victim's clock via a Sybil attack. This issue exists because of an incomplete fix for CVE ID : CVE-2016-1549. **CVE ID : CVE-2018-7170**	https://www.synology.com/support/security/Synology_SA_18_13	A-NTP-NTP-20418/152
DoS	06-03-2018	5	The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10. **CVE ID : CVE-2018-7182**	https://www.synology.com/support/security/Synology_SA_18_13	A-NTP-NTP-20418/153
Opencv					
Opencv					
DoS	05-03-2018	5	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (pixels <= (1<<30)) may be false. **CVE ID : CVE-2018-7714**	https://github.com/xiaoqx/pocs/tree/master/opencv/dos-by-assert	A-OPE-OPENC-20418/154
DoS	05-03-2018	5	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.width <= (1<<20)) may be false. **CVE ID : CVE-2018-7713**	https://github.com/xiaoqx/pocs/tree/master/opencv/dos-by-assert	A-OPE-OPENC-20418/155
DoS	05-03-2018	5	The validateInputImageSize function in modules/imgcodecs/src/loadsave.cpp in OpenCV 3.4.1 allows remote attackers to cause a denial of service (assertion failure) because (size.height <= (1<<20)) may be false. **CVE ID : CVE-2018-7712**	https://github.com/xiaoqx/pocs/tree/master/opencv/dos-by-assert	A-OPE-OPENC-20418/156
Openjpeg					
Openjpeg					
Overflow	02-03-2018	7.5	An issue was discovered in	NA	A-OPE-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			mj2/opj_mj2_extract.c in OpenJPEG 2.3.0. The output prefix was not checked for length, which could overflow a buffer, when providing a prefix with 50 or more characters on the command line. **CVE ID : CVE-2018-7648**		OPENJ-20418/157
Opensuse					
Cryptctl					
NA	01-03-2018	8.5	In cryptctl before version 2.0 a malicious server could send RPC requests that could overwrite files outside of the cryptctl key database. **CVE ID : CVE-2017-9270**	https://www.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-9270/	A-OPE-CRYPT-20418/158
Libzypp					
NA	01-03-2018	7.5	In libzypp before August 2018 GPG keys attached to YUM repositories were not correctly pinned, allowing malicious repository mirrors to silently downgrade to unsigned repositories with potential malicious content. **CVE ID : CVE-2017-9269**	https://www.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-9269/	A-OPE-LIBZY-20418/159
NA	01-03-2018	9.3	In libzypp before 20170803 it was possible to retrieve unsigned packages without a warning to the user which could lead to man in the middle or malicious servers to inject malicious RPM packages into a users system. **CVE ID : CVE-2017-7436**	https://www.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-7436/	A-OPE-LIBZY-20418/160
NA	01-03-2018	9.3	In libzypp before 20170803 it was possible to add unsigned YUM repositories without warning to the user that could lead to man in the middle or malicious servers to inject malicious RPM packages into a users system. **CVE ID : CVE-2017-7435**	https://www.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-7435/	A-OPE-LIBZY-20418/161
Open Build Service					
Gain	01-03-2018	5	The bs_worker code in open build service	https://ww	A-OPE-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Information			before 20170320 followed relative symlinks, allowing reading of files outside of the package source directory during build, allowing leakage of private information. **CVE ID : CVE-2017-5188**	w.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-5188/	OPEN - 20418/162
Otrs					
Otrs					
Execute Code	04-03-2018	9	** DISPUTED ** In the Admin Package Manager in Open Ticket Request System (OTRS) 5.0.0 through 5.0.24 and 6.0.0 through 6.0.1, authenticated admins are able to exploit a Blind Remote Code Execution vulnerability by loading a crafted opm file with an embedded CodeInstall element to execute a command on the server during package installation. NOTE: the vendor disputes this issue stating "the behaviour is as designed and needed for different packages to be installed", "there is a security warning if the package is not verified by OTRS Group", and "there is the possibility and responsibility of an admin to check packages before installation which is possible as they are not binary." **CVE ID : CVE-2018-7567**	https://0day.today/exploit/29938	A-OTR-OTRS-20418/163
Ovirt					
Ovirt					
Gain Information	06-03-2018	3.5	A vulnerability was discovered in oVirt 4.1.x before 4.1.9, where the combination of Enable Discard and Wipe After Delete flags for VM disks managed by oVirt, could cause a disk to be incompletely zeroed when removed from a VM. If the same storage blocks happen to be later allocated to a new disk attached to another VM, potentially sensitive data could be revealed to privileged users of that VM. **CVE ID : CVE-2018-1062**	https://gerrit.ovirt.org/#/c/84861/	A-OVI-OVIRT-20418/164
Piwigo					

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
Piwigo					
XSS Cross-Site Request Forgery	06-03-2018	3.5	The management panel in Piwigo 2.9.3 has stored XSS via the name parameter in a /admin.php?page=photo-${photo_number} request. CSRF exploitation, related to CVE ID : CVE-2017-10681, may be possible. **CVE ID : CVE-2018-7724**	https://github.com/summ3rf/Vulner/blob/master/Piwigo%20Store%20XSS.md	A-PIW-PIWIG-20418/165
XSS Cross-Site Request Forgery	06-03-2018	3.5	The management panel in Piwigo 2.9.3 has stored XSS via the virtual_name parameter in a /admin.php?page=cat_list request, a different issue than CVE ID : CVE-2017-9836. CSRF exploitation, related to CVE ID : CVE-2017-10681, may be possible. **CVE ID : CVE-2018-7723**	https://github.com/summ3rf/Vulner/blob/master/Piwigo%20Store%20XSS.md	A-PIW-PIWIG-20418/166
XSS Cross-Site Request Forgery	06-03-2018	3.5	The management panel in Piwigo 2.9.3 has stored XSS via the name parameter in a /ws.php?format=json request. CSRF exploitation, related to CVE ID : CVE-2017-10681, may be possible. **CVE ID : CVE-2018-7722**	https://github.com/summ3rf/Vulner/blob/master/Piwigo%20Store%20XSS.md	A-PIW-PIWIG-20418/167
Podofo Project					
Podofo					
Overflow	09-03-2018	6.8	In PoDoFo 0.9.5, there exists an infinite loop vulnerability in PdfParserObject::ParseFileComplete() in PdfParserObject.cpp which may result in stack overflow. Remote attackers could leverage this vulnerability to cause a denial-of-service or possibly unspecified other impact via a crafted pdf file. **CVE ID : CVE-2018-8002**	https://bugzilla.redhat.com/show_bug.cgi?id=1548930	A-POD-PODOF-20418/168
NA	09-03-2018	6.8	In PoDoFo 0.9.5, there exists a heap-based buffer over-read vulnerability in UnescapeName() in PdfName.cpp. Remote attackers could leverage this vulnerability to cause a denial-of-service or possibly unspecified other impact via a crafted pdf file. **CVE ID : CVE-2018-8001**	https://bugzilla.redhat.com/show_bug.cgi?id=1549469	A-POD-PODOF-20418/169
Execute Code Overflow	09-03-2018	6.8	In PoDoFo 0.9.5, there exists a heap-based buffer overflow vulnerability in PoDoFo::PdfTokenizer:: GetNext Token ()	https://bugzilla.redhat.com/show_b	A-POD-PODOF-20418/

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			in PdfTokenizer.cpp, a related issue to CVE-2017-5886. Remote attackers could leverage this vulnerability to cause a denial-of-service or potentially execute arbitrary code via a crafted pdf file. **CVE ID : CVE-2018-8000**	ug.cgi?id=1548918	170
Postgresql					
Postgresql					
Execute Code	02-03-2018	6.5	A flaw was found in the way Postgresql allowed a user to modify the behavior of a query for other users. An attacker with a user account could use this flaw to execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected. **CVE ID : CVE-2018-1058**	https://www.postgresql.org/about/news/1834/	A-POS-POSTG-20418/171
Privatevpn					
Privatevpn					
Execute Code	05-03-2018	10	PrivateVPN 2.0.31 for macOS suffers from a root privilege escalation vulnerability with its com.privat.vpn.helper privileged helper tool. This privileged helper tool implements an XPC service that allows arbitrary installed applications to connect and send messages. The XPC service extracts the config string from the corresponding XPC message. This string is supposed to point to an internal OpenVPN configuration file. If a new connection has not already been established, an attacker can send the XPC service a malicious XPC message with the config string pointing at an OpenVPN configuration file that he or she controls. In the configuration file, an attacker can specify a dynamic library plugin that should run for every new VPN connection. This plugin will execute code in the context of the root user. **CVE ID : CVE-2018-7716**	https://github.com/VerSprite/research/edit/master/advisories/VS-2018-006.md	A-PRI-PRIVA-20418/172
Execute Code	05-03-2018	10	PrivateVPN 2.0.31 for macOS suffers from a root privilege escalation vulnerability with its com.privat.vpn.helper privileged	https://github.com/VerSprite/resea	A-PRI-PRIVA-20418/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			helper tool. This privileged helper tool implements an XPC service that allows arbitrary installed applications to connect and send messages. The XPC service extracts the path string from the corresponding XPC message. This string is supposed to point to PrivateVPN's internal openvpn binary. If a new connection has not already been established, an attacker can send the XPC service a malicious XPC message with the path string pointing at a binary that he or she controls. This results in the execution of arbitrary code as the root user. **CVE ID : CVE-2018-7715**	rch/blob/master/advisories/VS-2018-005.md	173
Projectsend					
Projectsend					
XSS	06-03-2018	4.3	Cross-site scripting (XSS) vulnerability in ProjectSend (formerly cFTP) before commit 6c3710430be26feb5371cb0377e5355d6f9a27ca allows remote attackers to inject arbitrary web script or HTML via the Description field in My account Name updated, related to home.php and actions-log.php.**CVE ID : CVE-2017-9786**	https://github.com/ignacionelson/ProjectSend/pull/448/commits/6c3710430be26feb5371cb0377e5355d6f9a27ca	A-PRO-PROJE-20418/174
XSS	06-03-2018	4.3	Cross-site scripting (XSS) vulnerability in ProjectSend (formerly cFTP) before commit 6c3710430be26feb5371cb0377e5355d6f9a27ca allows remote attackers to inject arbitrary web script or HTML via the Description field in a Site name updated. **CVE ID : CVE-2017-9783**	https://github.com/ignacionelson/ProjectSend/compare/448/commits	A-PRO-PROJE-20418/175
Python					
Python					
DoS	01-03-2018	4.3	** DISPUTED ** The Wave_read._read_fmt_chunk function in Lib/wave.py in Python through 3.6.4 does not ensure a nonzero channel value, which allows attackers to cause a denial of service (divide-by-zero and exception)	https://bugs.python.org/issue32056	A-PYT-PYTHO-20418/176

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			via a crafted wav format audio file. NOTE: the vendor disputes this issue because Python applications "need to be prepared to handle a wide variety of exceptions." **CVE ID : CVE-2017-18207**		
Execute Code Overflow	07-03-2018	7.2	Python Software Foundation CPython version From 3.2 until 3.6.4 on Windows contains a Buffer Overflow vulnerability in os.symlink() function on Windows that can result in Arbitrary code execution, likely escalation of privilege. This attack appears to be exploitable via a python script that creates a symlink with an attacker controlled name or location. This vulnerability appears to have been fixed in 3.7.0 and 3.6.5. **CVE ID : CVE-2018-1000117**	https://github.com/python/cpython/pull/5989	A-PYT-PYTHO-20418/177
Qcms					
Qcms					
XSS	2018-03-12	3.5	QCMS version 3.0 has XSS via the title parameter to the /guest/index.html URI. **CVE ID : CVE-2018-8070**	https://github.com/imsebao/404team/blob/master/qcms_xss/qcms_xss.md	A-QCM-QCMS-20418/178
XSS	2018-03-12	3.5	QCMS version 3.0 has XSS via the webname parameter to the /backend/system.html URI. **CVE ID : CVE-2018-8069**	https://github.com/imsebao/404team/blob/master/qcms/qcms.md	A-QCM-QCMS-20418/179
Qemu					
Qemu					
Execute Code	01-03-2018	4.6	The load_multiboot function in hw/i386/multiboot.c in Quick Emulator (aka QEMU) allows local guest OS users to execute arbitrary code on the QEMU host via a mh_load_end_addr value greater than mh_bss_end_addr, which triggers an out-of-bounds read or write memory access. **CVE ID : CVE-2018-7550**	https://bugzilla.redhat.com/show_bug.cgi?id=1549798	A-QEM-QEMU-20418/180

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Qnap					
Media Streaming Add-on					
XSS	08-03-2018	4.3	Cross-site scripting (XSS) vulnerability in QNAP NAS application Media Streaming add-on version 421.1.0.2, 430.1.2.0, and earlier allows remote attackers to inject arbitrary web script or HTML. The injected code will only be triggered by a crafted link, not the normal page. **CVE ID : CVE-2017-7634**	https://www.qnap.com/zh-tw/security-advisory/nas-201803-08	A-QNA-MEDIA-20418/181
Gain Information	08-03-2018	6.4	QNAP NAS application Media Streaming add-on version 421.1.0.2, 430.1.2.0, and earlier does not authenticate requests properly. Successful exploitation could lead to change of the Media Streaming settings, and leakage of sensitive information of the QNAP NAS. **CVE ID : CVE-2017-7638**	https://www.qnap.com/zh-tw/security-advisory/nas-201803-08	A-QNA-MEDIA-20418/182
Cross-Site Request Forgery	08-03-2018	6.8	QNAP NAS application Media Streaming add-on version 421.1.0.2, 430.1.2.0, and earlier does not utilize CSRF protections. **CVE ID : CVE-2017-7641**	https://www.qnap.com/zh-tw/security-advisory/nas-201803-08	A-QNA-MEDIA-20418/183
Gain privileges	08-03-2018	10	QNAP NAS application Media Streaming add-on version 421.1.0.2, 430.1.2.0, and earlier allows remote attackers to run arbitrary OS commands against the system with root privileges. **CVE ID : CVE-2017-7640**	https://www.qnap.com/zh-tw/security-advisory/nas-201803-08	A-QNA-MEDIA-20418/184
Qfinder Pro					
Gain Information	05-03-2018	5	QNAP Qfinder Pro 6.1.0.0317 and earlier may expose sensitive information contained in NAS devices. If exploited, this may allow attackers to further compromise the device. **CVE ID : CVE-2017-7633**	https://www.qnap.com/zh-tw/security-advisory/nas-201802-27	A-QNA-QFIND-20418/185
Rapidscada					
Rapid Scada					
Execute Code	08-03-2018	7.2	A vulnerability allows local attackers to	NA	A-RAP-

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			escalate privilege on Rapid Scada 5.5.0 because of weak C:\SCADA permissions. The specific flaw exists within the access control that is set and modified during the installation of the product. The product sets weak access control restrictions. An attacker can leverage this vulnerability to execute arbitrary code under the context of Administrator, the IUSR account, or SYSTEM. **CVE ID : CVE-2018-5313**		RAPID-20418/ 186
Redhat					
Openshift					
NA	09-03-2018	5.4	Red Hat OpenShift Enterprise version 3.7 is vulnerable to access control override for container network filesystems. An attacker could override the UserId and GroupId for GlusterFS and NFS to read and write any data on the network filesystem. **CVE ID : CVE-2018-1069**	https://bugzilla.redhat.com/show_bug.cgi?id=1552987	A-RED-OPENS-20418/ 187
Resteasy					
Execute Code	09-03-2018	6.8	JBoss RESTEasy before version 3.1.2 could be forced into parsing a request with YamlProvider, resulting in unmarshalling of potentially untrusted data which could allow an attacker to execute arbitrary code with RESTEasy application permissions. **CVE ID : CVE-2016-9606**	https://bugzilla.redhat.com/show_bug.cgi?id=1400644	A-RED-RESTE-20418/ 188
Samsung					
Display Solutions					
NA	06-03-2018	4.3	Samsung Display Solutions App before 3.02 for Android allows man-in-the-middle attackers to spoof B2B content by leveraging failure to use encryption during information transmission. **CVE ID : CVE-2018-6019**	https://wws.nightwatchcybersecurity.com/2018/03/01/content-injection-in-samsung-display-solutions-application-for-android-	A-SAM-DISPL-20418/ 189

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
				CVE-2018-6019/	
SAP					
Business Application Software Integrated Solution					
Directory Traverse	01-03-2018	6.5	ABAP File Interface in, SAP BASIS, from 7.00 to 7.02, from 7.10 to 7.11, 7.30, 7.31, 7.40, from 7.50 to 7.52, allows an attacker to exploit insufficient validation of path information provided by users, thus characters representing "traverse to parent directory" are passed through to the file APIs.**CVE ID : CVE-2018-2367**	https://launchpad.support.sap.com/#/notes/2562089	A-SAP-BUSIN-20418/190
Customer Relationship Management					
Directory Traverse	01-03-2018	6.5	SAP CRM, 7.01, 7.02,7.30, 7.31, 7.33, 7.54, allows an attacker to exploit insufficient validation of path information provided by users, thus characters representing "traverse to parent directory" are passed through to the file APIs. **CVE ID : CVE-2018-2380**	https://launchpad.support.sap.com/#/notes/2547431	A-SAP-CUSTO-20418/191
Netweaver Portal					
XSS	01-03-2018	4.3	SAP NetWeaver Portal, WebDynpro Java, 7.30, 7.31, 7.40, 7.50, does not sufficiently encode user controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2018-2365**	https://launchpad.support.sap.com/#/notes/2547977	A-SAP-NETWE-20418/192
Netweaver System Landscape Directory					
NA	01-03-2018	7.5	SAP NetWeaver System Landscape Directory, LM-CORE 7.10, 7.20, 7.30, 7.31, 7.40, does not perform any authentication checks for functionalities that require user identity. **CVE ID : CVE-2018-2368**	https://launchpad.support.sap.com/#/notes/2565622	A-SAP-NETWE-20418/193
Schneider-electric					
Somove					
Execute Code	09-03-2018	6.8	A DLL hijacking vulnerability exists in Schneider Electric's SoMove Software and associated DTM software components in all versions prior to 2.6.2 which could allow an attacker to execute arbitrary code. **CVE ID : CVE-2018-7239**	https://www.schneider-electric.com/en/download/document/SEVD-2018-060-	A-SCH-SOMOV-20418/194

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
				01/	
Segger					
Embos/ip Ftp Server					
DoS	03-03-2018	5	SEGGER embOS/IP FTP Server 3.22 allows remote attackers to cause a denial of service (daemon crash) via an invalid LIST, STOR, or RETR command. **CVE ID : CVE-2018-7449**	https://www.exploit-db.com/exploits/44221/	A-SEG-EMBOS-20418/195
SIL					
Graphite2					
DoS	09-03-2018	6.8	In libgraphite2 in graphite2 1.3.11, a NULL pointer dereference vulnerability was found in Segment.cpp during a dumbRendering operation, which may allow attackers to cause a denial of service or possibly have unspecified other impact via a crafted .ttf file. **CVE ID : CVE-2018-7999**	NA	A-SIL-GRAPH-20418/196
Simplesamlphp					
Simplesamlphp					
NA	05-03-2018	5	The XmlSecLibs library as used in the saml2 library in SimpleSAMLphp before 1.15.3 incorrectly verifies signatures on SAML assertions, allowing a remote attacker to construct a crafted SAML assertion on behalf of an Identity Provider that would pass as cryptographically valid, thereby allowing them to impersonate a user from that Identity Provider, aka a key confusion issue. **CVE ID : CVE-2018-7644**	https://simplesamlphp.org/security/201802-01	A-SIM-SIMPL-20418/197
Sinatrarb					
Sinatra					
Gain Information CSRF	07-03-2018	4.3	Sinatra rack-protection versions 1.5.4 and 2.0.0.rc3 and earlier contains a timing attack vulnerability in the CSRF token checking that can result in signatures can be exposed. This attack appear to be exploitable via network connectivity to the ruby application. This vulnerability appears to have been fixed in 1.5.5 and 2.0.0.	https://github.com/sinatra/sinatra/commit/8aa6c42ef724f93ae309fb7c5668e19ad547eceb#commitcomme	A-SIN-SINAT-20418/198

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-1000119	nt-27964109	
Soflyy					
Wp All Import					
XSS	09-03-2018	4.3	Cross-site scripting vulnerability in WP All Import plugin prior to version 3.4.7 for WordPress allows an attacker to inject arbitrary web script or HTML via unspecified vectors. **CVE ID : CVE-2018-0547**	https://wordpress.org/plugins/wp-all-import/#developers	A-SOF-WPAL-20418/199
Suse					
Open Build Service					
DoS	01-03-2018	4	In the open build service before 201707022 the wipetrigger and rebuild actions checked the wrong project for permissions, allowing authenticated users to cause operations on projects where they did not have permissions leading to denial of service (resource consumption).**CVE ID : CVE-2017-9268**	https://github.com/openSUSE/open-build-service/pull/3267	A-SUS-OPEN -20418/200
Testlink					
Testlink					
Gain Information	05-03-2018	5	TestLink through 1.9.16 allows remote attackers to read arbitrary attachments via a modified ID field to /lib/attachments/attachmentdownload.php. **CVE ID : CVE-2018-7668**	http://lists.openwall.net/full-disclosure/2018/02/28/1	A-TES-TESTL-20418/201
Thycotic					
Secret Server					
NA	09-03-2018	7.5	The Remote Desktop Launcher in Thycotic Secret Server before 8.6.000010 does not properly cleanup a temporary file that contains an encrypted password once a session has ended. **CVE ID : CVE-2014-4861**	http://thycotic.com/products/secret-server/resources/advisories/CVE ID : CVE-2014-4861/	A-THY-SECRE-20418/202
Tiki					
Tikiwiki Cms/groupware					
XSS	09-03-2018	3.5	Cross Site Scripting (XSS) exists in Tiki	https://sour	A-TIK-

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			before 12.13, 15.6, 17.2, and 18.1. **CVE ID : CVE-2018-7290**	ceforge.net/p/tikiwiki/code/65537	TIKIW-20418/203
Torproject					
TOR					
DoS	05-03-2018	5	An issue was discovered in Tor before 0.2.9.15, 0.3.1.x before 0.3.1.10, and 0.3.2.x before 0.3.2.10. The directory-authority protocol-list subprotocol implementation allows remote attackers to cause a denial of service (NULL pointer dereference and directory-authority crash) via a misformatted relay descriptor that is mishandled during voting. **CVE ID : CVE-2018-0490**	https://blog.torproject.org/new-stable-tor-releases-security-fixes-and-dos-prevention-03210-03110-02915	A-TOR-TOR-20418/204
Util-linux Project					
Util-linux					
Gain Privileges	06-03-2018	7.2	In util-linux before 2.32-rc1, bash-completion/umount allows local users to gain privileges by embedding shell commands in a mountpoint name, which is mishandled during a umount command (within Bash) by a different user, as demonstrated by logging in as root and entering umount followed by a tab character for auto completion. **CVE ID : CVE-2018-7738**	NA	A-UTI-UTIL--20418/205
Weblogexpert					
Weblog Expert					
NA	09-03-2018	4.6	\ProgramData\WebLog Expert\WebServer\WebServer.cfg in WebLog Expert Web Server Enterprise 9.4 has weak permissions (BUILTIN\Users:(ID)C), which allows local users to set a cleartext password and login as admin. **CVE ID : CVE-2018-7581**	NA	A-WEB-WEBLO-20418/206
DoS	09-03-2018	5	WebLog Expert Web Server Enterprise 9.4 allows Remote Denial Of Service (daemon crash) via a long HTTP Accept Header to TCP port 9991.	NA	A-WEB-WEBLO-20418/207

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-7582		
Westernbridgegroup					
Razor					
XSS	07-03-2018	4.3	An issue was discovered in Western Bridge Cobub Razor 0.7.2. Authentication is not required for /index.php?/manage/channel/modifychannel. For example, with a crafted channel name, stored XSS is triggered during a later /index.php?/manage/channel request by an admin. **CVE ID : CVE-2018-7746**	https://github.com/cobub/razor/issues/161	A-WES-RAZOR-20418/208
NA	07-03-2018	5	An issue was discovered in Western Bridge Cobub Razor 0.7.2. Authentication is not required for /index.php?/install/installation/createuserinfo requests, resulting in account creation. **CVE ID : CVE-2018-7745**	https://github.com/cobub/razor/issues/161	A-WES-RAZOR-20418/209
Cross-Site Request Forgery	07-03-2018	6.8	A cross-site request forgery (CSRF) vulnerability exists in Western Bridge Cobub Razor 0.7.2 via /index.php?/user/createNewUser/, resulting in account creation. **CVE ID : CVE-2018-7720**	https://github.com/Kyhvedn/CVE ID : CVE_Description/blob/master/CVE ID : CVE-2018-7720_Description.md	A-WES-RAZOR-20418/210
Windows Optimization Master Project					
Windows Optimization Master					
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002004. **CVE ID : CVE-2018-8997**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002004	A-WIN-WINDO-20418/211
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows	https://github.com/D0neMkj/POC_B	A-WIN-WINDO-20418/

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002007. **CVE ID : CVE-2018-8996**	SOD/tree/master/Windows%20Optimization%20master/0xf1002007	212
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002002. **CVE ID : CVE-2018-8995**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002002	A-WIN-WINDO-20418/213
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002003. **CVE ID : CVE-2018-8994**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002003	A-WIN-WINDO-20418/214
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002001. **CVE ID : CVE-2018-8993**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002001	A-WIN-WINDO-20418/215
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002005. **CVE ID : CVE-2018-8992**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002005	A-WIN-WINDO-20418/216
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the	https://github.com/D0n	A-WIN-WINDO-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002009. **CVE ID : CVE-2018-8991**	eMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002009	20418/217
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002010. **CVE ID : CVE-2018-8990**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002010	A-WIN-WINDO-20418/218
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002006. **CVE ID : CVE-2018-8989**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002006	A-WIN-WINDO-20418/219
DoS	24-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002008. **CVE ID : CVE-2018-8988**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002008	A-WIN-WINDO-20418/220
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100284c. **CVE ID : CVE-2018-9054**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100284c	A-WIN-WINDO-20418/221
DoS	26-03-2018	6.1	In Windows Master (aka Windows	https://gith	A-WIN-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf10026cc. **CVE ID : CVE-2018-9053**	ub.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf10026cc	WINDO-20418/222
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100283c. **CVE ID : CVE-2018-9052**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100283c	A-WIN-WINDO-20418/223
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002021. **CVE ID : CVE-2018-9051**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002021	A-WIN-WINDO-20418/224
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100202d. **CVE ID : CVE-2018-9050**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100202D	A-WIN-WINDO-20418/225
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002833. **CVE ID : CVE-2018-9049**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002833	A-WIN-WINDO-20418/226

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100282c. **CVE ID : CVE-2018-9048**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100282C	A-WIN-WINDO-20418/227
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002841. **CVE ID : CVE-2018-9047**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002841	A-WIN-WINDO-20418/228
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf100282d. **CVE ID : CVE-2018-9046**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf100282d	A-WIN-WINDO-20418/229
DoS	26-03-2018	6.1	In Windows Master (aka Windows Optimization Master) 7.99.13.604, the driver file (WoptiHWDetect.SYS) allows local users to cause a denial of service (BSOD) or possibly have unspecified other impact because of not validating input values from IOCtl 0xf1002849. **CVE ID : CVE-2018-9045**	https://github.com/D0neMkj/POC_BSOD/tree/master/Windows%20Optimization%20master/0xf1002849	A-WIN-WINDO-20418/230
Woodybells					
Jtrim					
Gain Privileges	09-03-2018	9.3	Untrusted search path vulnerability in Jtrim 1.53c and earlier (Installer) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2018-0543**	http://woodybells.com/jtrim.html	A-WOO-JTRIM-20418/231

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Winshot					
Gain Privileges	09-03-2018	9.3	Untrusted search path vulnerability in WinShot 1.53a and earlier (Installer) allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. **CVE ID : CVE-2018-0544**	NA	A-WOO-WINSH-20418/232
Yxtcmf					
Yxtcmf					
Cross-Site Request Forgery	06-03-2018	6.8	An issue was discovered in YxtCMF 3.1. RbacController.class.php has CSRF, as demonstrated by modifying an administrator account via index.php/admin/user/add_post.html. **CVE ID : CVE-2018-7733**	https://github.com/SQYY/CVE ID : CVE/blob/master/YxtCMF_C	A-YXT-YXTCM-20418/233
Sql	06-03-2018	7.5	An issue was discovered in YxtCMF 3.1. SQL Injection exists in ShitiController.class.php via the ids array parameter to exam/shiti/delshiti.html. **CVE ID : CVE-2018-7732**	https://github.com/SQYY/CVE ID : CVE/blob/master/YxtCMF_S.txt	A-YXT-YXTCM-20418/234
Yzmcms					
Yzmcms					
XSS	13-03-2018	3.5	YzmCMS 3.7 has Stored XSS via the title parameter to advertisement/adver/edit.html. **CVE ID : CVE-2018-8078**	https://github.com/AlwaysHereFight/YZMCMSxss/blob/master/README.md	A-YZM-YZMCM-20418/235
Sql	01-03-2018	6.5	\application\admin\controller\update_urls .class.php in YzmCMS 3.6 has SQL Injection via the catids array parameter to admin/update_urls/update_category_url.html. **CVE ID : CVE-2018-7579**	http://www.atksec.com/article/yzmcms-v3.6-sqli/index.html	A-YZM-YZMCM-20418/236
Yzmcms Project					
Yzmcms					
XSS	04-03-2018	4.3	In YzmCMS 3.6, index.php has XSS via the a, c, or m parameter. **CVE ID : CVE-2018-7653**	https://github.com/ponyma233/YzmCMS/blob/master/YzmCMS_3.6_b	A-YZM-YZMCM-20418/237

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
				ug.md	
Zblogcn					
Z-blogphp					
XSS	06-03-2018	4.3	In Z-BlogPHP 1.5.1.1740, cmd.php has XSS via the ZC_BLOG_SUBNAME parameter or ZC_UPLOAD_FILETYPE parameter. **CVE ID : CVE-2018-7736**	https://github.com/ponyma233/cms/blob/master/Z-Blog_1.5.1.1740_bugs.md	A-ZBL-Z-BLO-20418/238
Gain Information	06-03-2018	5	In Z-BlogPHP 1.5.1.1740, there is Web Site physical path leakage, as demonstrated by admin_footer.php or admin_footer.php. **CVE ID : CVE-2018-7737**	https://github.com/ponyma233/cms/blob/master/Z-Blog_1.5.1.1740_bugs.md#web-site-physical-path-leakage	A-ZBL-Z-BLO-20418/239
Zonemaster Project					
Zonemaster Web Gui					
XSS	03-03-2018	4.3	lib/Zonemaster/GUI/Dancer/Export.pm in Zonemaster Web GUI before 1.0.11 has XSS. **CVE ID : CVE-2018-7652**	https://github.com/dotse/zonemaster-gui/releases/tag/v1.0.11	A-ZON-ZONEM-20418/240
Zziplib Project					
Zziplib					
DoS Overflow	06-03-2018	4.3	An issue was discovered in ZZIPlib 0.13.68. There is a memory leak triggered in the function zzip_mem_disk_new in memdisk.c, which will lead to a denial of service attack. **CVE ID : CVE-2018-7727**	https://github.com/gdraheim/zziplib/issues/40	A-ZZI-ZZIPL-20418/241
DoS Overflow	06-03-2018	4.3	An issue was discovered in ZZIPlib 0.13.68. There is a bus error caused by the __zzip_parse_root_directory function of zip.c. Attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.	https://github.com/gdraheim/zziplib/issues/41	A-ZZI-ZZIPL-20418/242

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2018-7726		
DoS Overflow	06-03-2018	4.3	An issue was discovered in ZZIPlib 0.13.68. An invalid memory address dereference was discovered in zzip_disk_fread in mmapped.c. The vulnerability causes an application crash, which leads to denial of service. **CVE ID : CVE-2018-7725**	https://github.com/gdraheim/zziplib/issues/39	A-ZZI-ZZIPL-20418/243
Application;Operating System					
Apache/Redhat					
Http Server/Enterprise Linux					
NA	09-03-2018	3.3	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process. **CVE ID : CVE-2016-8612**	https://bugzilla.redhat.com/show_bug.cgi?id=1387605	A-APA-HTTP -20418/244
Cavium;Cisco/Cisco					
Nitrox Ssl Sdk;Nitrox V Ssl Sdk;Octeon Sdk;Octeon Ssl Sdk;Turbossl Sdk/Webex Conect Im;Webex Meetings/Ace30 Application Control Engine Module Firmware;Ace4710 Application Control Engine Firmware;Adaptive Security Appliance 5505 Firmware;Adaptive Security Appliance 5510 Firmware;Adaptive Security Appliance 5520 Firmware;Adaptive Security Appliance 5540 Firmware;Adaptive Security Appliance 5550 Firmware					
Gain Information	05-03-2018	7.1	Cavium Nitrox SSL, Nitrox V SSL, and TurboSSL software development kits (SDKs) allow remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a ROBOT attack.**CVE ID : CVE-2017-17428**	https://www.cavium.com/security-advisory-CVE-2017-17428.html	A-CAV-NITRO-20418/245
Fedoraproject/Redhat					
389 Directory Server/Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Workstation					
DoS	07-03-2018	5	An out-of-bounds memory read flaw was found in the way 389-ds-base handled certain LDAP search filters, affecting all versions including 1.4.x. A remote, unauthenticated attacker could potentially use this flaw to make ns-slapd crash via a specially crafted LDAP request, thus resulting in denial of service. **CVE ID : CVE-2018-1054**	https://bugzilla.redhat.com/show_bug.cgi?id=1537314	A-FED-389D-20418/246
NTP;Synology/Slackware;Synology					

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
NTP/Diskstation Manager;Router Manager;Skynas;Virtual Diskstation Manager/Slackware Linux/ Vs960hd Firmware					
DoS	06-03-2018	5	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association. **CVE ID : CVE-2018-7185**	https://www.synology.com/support/security/Synology_SA_18_13	A-NTP-NTP/D-20418/247
DoS	06-03-2018	5	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE ID : CVE-2015-7704. **CVE ID : CVE-2018-7184**	https://www.synology.com/support/security/Synology_SA_18_13	A-NTP-NTP/D-20418/248
PHP/Ubuntu					
PHP/Ubuntu					
Overflow	01-03-2018	7.5	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_ wrapper.c. This subsequently results in copying a large string. **CVE ID : CVE-2018-7584**	https://github.com/php/php-src/commit/523f230c831d7b33353203fa34aee4e92ac12bba	A-PHP-PHP/U-20418/249
Postgresql/Suse					
Postgresql/Suse Linux Enterprise Server					
NA	01-03-2018	6.9	A race condition in the postgresql init script could be used by attackers able to access the postgresql account to escalate their privileges to root. **CVE ID : CVE-2017-14798**	https://www.suse.com/de-de/security/CVE-2017-14798/	A-POS-POSTG-20418/250
Hardware					
Belden					

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
Hirschmann M1-8mm-sc;Hirschmann M1-8sfp;Hirschmann M1-8sm-sc;Hirschmann M1-8tp-rj45;Hirschmann Mach102-24tp-f;Hirschmann Mach102-24tp-fr;Hirschmann Mach102-8tp;Hirschmann Mach102-8tp-f;Hirschmann Mach102-8tp-fr;Hirschmann Mach102-8tp-r;Hirschmann Mach104-16tx-poep;Hirschmann Mach104-16tx-poep +2x;Hirschmann Mach104-16tx-poep +2x -e;Hirschmann Mach104-16tx-poep +2x -e-l3p;Hirschmann Mach104-16tx-poep +2x -r;Hirschmann Mach104-16tx-poep +2x -r-l3p;Hirschmann Mach104-16tx-poep +2x-l3p;Hirschmann Mach104-16tx-poep -e;Hirschmann Mach104-16tx-poep -e-l3p;Hirschmann Mach104-16tx-poep -r;Hirschmann Mach104-16tx-poep -r-l3p;Hirschmann Mach104-16tx-poep-l3p;Hirschmann Mach104-20tx-f;Hirschmann Mach104-20tx-f-4poe;Hirschmann Mach104-20tx-f-l3p;Hirschmann Mach104-20tx-fr;Hirschmann Mach104-20tx-fr-l3p;Hirschmann Mach4002-24g+3x-l2p;Hirschmann Mach4002-24g+3x-l3e;Hirschmann Mach4002-24g+3x-l3p;Hirschmann Mach4002-24g-l2p;Hirschmann Mach4002-24g-l3e;Hirschmann Mach4002-24g-l3p;Hirschmann Mach4002-48g+3x-l2p;Hirschmann Mach4002-48g+3x-l3e;Hirschmann Mach4002-48g+3x-l3p;Hirschmann Mach4002-48g-l2p;Hirschmann Mach4002-48g-l3e;Hirschmann Mach4002-48g-l3p;Hirschmann Ms20-0800eccp;Hirschmann Ms20-0800saae;Hirschmann Ms20-0800saap;Hirschmann Ms20-1600eccp;Hirschmann Ms20-1600saae;Hirschmann Ms20-1600saap;Hirschmann Ms30-0802saae;Hirschmann Ms30-0802saap;Hirschmann Ms30-1602saae;Hirschmann Octopus 16m;Hirschmann Octopus 16m-8poe;Hirschmann Octopus 16m-train;Hirschmann Octopus 16m-train-bp;Hirschmann Octopus 24m;Hirschmann Octopus 24m-8 Poe;Hirschmann Octopus 24m-train;Hirschmann Octopus 24m-train-bp;Hirschmann Octopus 5tx Eec;Hirschmann Octopus 8m;Hirschmann Octopus 8m-6poe;Hirschmann Octopus 8m-8poe;Hirschmann Octopus 8m-train;Hirschmann Octopus 8m-train-bp;Hirschmann Octopus 8tx Poe-eec;Hirschmann Octopus 8tx-eec;Hirschmann Octopus Os20-000900t5t5tafbhh;Hirschmann Octopus Os20-000900t5t5tnebhh;Hirschmann Octopus Os20-0010001m1mtrephh;Hirschmann Octopus Os20-0010001s1strephh;Hirschmann Octopus Os20-0010004m4mtrephh;Hirschmann Octopus Os20-0010004s4strephh;Hirschmann Octopus Os20-001000t5t5tafuhb;Hirschmann Octopus Os20-001000t5t5tneuhb;Hirschmann Octopus Os24-080900t5t5tffbhh;Hirschmann Octopus Os24-080900t5t5tnebhh;Hirschmann Octopus Os24-081000t5t5tffuhb;Hirschmann Octopus Os24-081000t5t5tneuhb;Hirschmann Octopus Os30;Hirschmann Octopus Os30-0008021a1atrephh;Hirschmann Octopus Os30-0008021b1btrephh;Hirschmann Octopus Os30-0008024a4atrephh;Hirschmann Octopus Os30-0008024b4btrephh;Hirschmann Octopus Os32-080802o6o6tpephh;Hirschmann Octopus Os32-080802t6t6tpephh;Hirschmann Octopus Os32-081602o6o6tpephh;Hirschmann Octopus Os32-081602t6t6tpephh;Hirschmann Octopus Os34;Hirschmann Octopus Os3x-xx16xxx;Hirschmann Octopus Os3x-xx24xxx;Hirschmann Rs20-0900mmm2tdau;Hirschmann Rs20-0900nnm4tdau;Hirschmann Rs20-0900vvm2tdau;Hirschmann Rs20-1600l2l2sdau;Hirschmann Rs20-1600l2m2sdau;Hirschmann Rs20-1600l2s2sdau;Hirschmann Rs20-1600l2t1sdau;Hirschmann Rs20-1600m2m2sdau;Hirschmann Rs20-1600m2t1sdau;Hirschmann Rs20-1600s2m2sdau;Hirschmann Rs20-1600s2s2sdau;Hirschmann Rs20-1600s2t1sdau;Hirschmann Rsb20-0800m2m2saab;Hirschmann Rsb20-0800m2m2saabe;Hirschmann Rsb20-0800m2m2taab;Hirschmann Rsb20-0800m2m2taabe;Hirschmann Rsb20-0800s2s2saab;Hirschmann Rsb20-0800s2s2saabe;Hirschmann Rsb20-0800s2s2taab;Hirschmann Rsb20-0800s2s2taabe;Hirschmann Rsb20-0800t1t1saab;Hirschmann Rsb20-0800t1t1saabe;Hirschmann Rsb20-0800t1t1taab;Hirschmann Rsb20-0800t1t1taabe;Hirschmann Rsb20-0900m2ttsaab;Hirschmann Rsb20-0900m2ttsaabe;Hirschmann Rsb20-0900m2tttaab;Hirschmann Rsb20-0900m2tttaabe;Hirschmann Rsb20-0900mmm2saab;Hirschmann Rsb20-0900mmm2saabe;Hirschmann Rsb20-					

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
0900mmm2taab;Hirschmann Rsb20-0900mmm2taabe;Hirschmann Rsb20-0900s2ttsaab;Hirschmann Rsb20-0900s2ttsaabe;Hirschmann Rsb20-0900s2tttaab;Hirschmann Rsb20-0900s2tttaabe;Hirschmann Rsb20-0900vvm2saab;Hirschmann Rsb20-0900vvm2saabe;Hirschmann Rsb20-0900vvm2taab;Hirschmann Rsb20-0900vvm2taabe;Hirschmann Rsb20-0900zzz6saab;Hirschmann Rsb20-0900zzz6saabe;Hirschmann Rsb20-0900zzz6taab;Hirschmann Rsb20-0900zzz6taabe;Hirschmann Rsr20;Hirschmann Rsr30					
Gain Information	06-03-2018	4.3	A Cleartext Transmission of Sensitive Information issue was discovered in Belden Hirschmann RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, and OCTOPUS Classic Platform Switches. A cleartext transmission of sensitive information vulnerability in the web interface has been identified, which may allow an attacker to obtain sensitive information through a successful man-in-the-middle attack. **CVE ID : CVE-2018-5471**	NA	H-BEL-HIRSC-20418/251
Gain Information	06-03-2018	5.8	An Inadequate Encryption Strength issue was discovered in Belden Hirschmann RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, and OCTOPUS Classic Platform Switches. An inadequate encryption strength vulnerability in the web interface has been identified, which may allow an attacker to obtain sensitive information through a successful man-in-the-middle attack. **CVE ID : CVE-2018-5461**	NA	H-BEL-HIRSC-20418/252
NA	06-03-2018	6.4	An Information Exposure Through Query Strings in GET Request issue was discovered in Belden Hirschmann RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, and OCTOPUS Classic Platform Switches. An information exposure through query strings vulnerability in the web interface has been identified, which may allow an attacker to impersonate a legitimate user. **CVE ID : CVE-2018-5467**	NA	H-BEL-HIRSC-20418/253
NA	06-03-2018	6.8	A Session Fixation issue was discovered in Belden Hirschmann RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, and OCTOPUS Classic Platform Switches.	NA	H-BEL-HIRSC-20418/254

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			A session fixation vulnerability in the web interface has been identified, which may allow an attacker to hijack web sessions. **CVE ID : CVE-2018-5465**		
NA	06-03-2018	7.5	An Improper Restriction of Excessive Authentication Attempts issue was discovered in Belden Hirschmann RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, and OCTOPUS Classic Platform Switches. An improper restriction of excessive authentication vulnerability in the web interface has been identified, which may allow an attacker to brute force authentication. **CVE ID : CVE-2018-5469**	NA	H-BEL-HIRSC-20418/ 255
Operating System (OS)					
Buffalo					
Wxr-1900dhp2 Firmware					
Execute Code Overflow	09-03-2018	6.8	Buffer overflow in Buffalo WXR-1900DHP2 firmware Ver.2.48 and earlier allows an attacker to execute arbitrary code via a specially crafted file. **CVE ID : CVE-2018-0522**	http://buffalo.jp/support_s/s20180223.html	O-BUF-WXR-1-20418/ 256
Execute Code	09-03-2018	8.3	Buffalo WXR-1900DHP2 firmware Ver.2.48 and earlier allows an attacker to execute arbitrary OS commands via unspecified vectors. **CVE ID : CVE-2018-0523**	http://buffalo.jp/support_s/s20180223.html	O-BUF-WXR-1-20418/ 257
Execute Code Bypass	09-03-2018	8.3	Buffalo WXR-1900DHP2 firmware Ver.2.48 and earlier allows an attacker to bypass authentication and execute arbitrary commands on the device via unspecified vectors. **CVE ID : CVE-2018-0521**	http://buffalo.jp/support_s/s20180223.html	O-BUF-WXR-1-20418/ 258
Cisco					
Asr 5000 Firmware;Asr 5500 Firmware;Asr 5700 Firmware					
Execute Code	08-03-2018	7.2	A vulnerability in the CLI of the Cisco StarOS operating system for Cisco ASR 5000 Series Aggregation Services Routers could allow an authenticated, local attacker to perform a command injection attack on an affected system. The vulnerability is due to insufficient	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-ASR 5-20418/ 259

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			validation of commands that are supplied to certain configurations in the CLI of the affected operating system. An attacker could exploit this vulnerability by injecting crafted arguments into a vulnerable CLI command for an affected system. A successful exploit could allow the attacker to insert and execute arbitrary commands in the CLI of the affected system. To exploit this vulnerability, the attacker would need to authenticate to an affected system by using valid administrator credentials. Cisco Bug IDs: CSCvg29441. **CVE ID : CVE-2018-0217**	20180307-staros	
Asyncos					
NA	08-03-2018	6.8	A vulnerability in the FTP server of the Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to log in to the FTP server of the device without a valid password. The attacker does need to have a valid username. The vulnerability is due to incorrect FTP user credential validation. An attacker could exploit this vulnerability by using FTP to connect to the management IP address of the targeted device. A successful exploit could allow the attacker to log in to the FTP server of the Cisco WSA without having a valid password. This vulnerability affects Cisco AsyncOS for WSA Software on both virtual and hardware appliances that are running any release of Cisco AsyncOS 10.5.1 for WSA Software. The device is vulnerable only if FTP is enabled on the management interface. FTP is disabled by default. Cisco Bug IDs: CSCvf74281. **CVE ID : CVE-2018-0087**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-wsa	O-CIS-ASYNC-20418/260
Ios Xe					
NA	2018-03-28	4	A vulnerability in the web-based user interface (web UI) of Cisco IOS XE	https://tools.cisco.com/	O-CIS-IOS X-20418/

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			Software could allow an authenticated, remote attacker to write arbitrary files to the operating system of an affected device. The vulnerability is due to insufficient input validation of HTTP requests that are sent to the web UI of the affected software. An attacker could exploit this vulnerability by sending a malicious HTTP request to the web UI of the affected software. A successful exploit could allow the attacker to write arbitrary files to the operating system of an affected device. Cisco Bug IDs: CSCvb22645.**CVE ID : CVE-2018-0196**	security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-wfw	261
Small Business 500 Series Stackable Managed Switches Firmware					
DoS	08-03-2018	6.8	A vulnerability in the Simple Network Management Protocol (SNMP) subsystem communication channel through the Cisco 550X Series Stackable Managed Switches could allow an authenticated, remote attacker to cause the device to reload unexpectedly, causing a denial of service (DoS) condition. The device nay need to be manually reloaded to recover. The vulnerability is due to lack of proper input throttling of ingress SNMP traffic over an internal interface. An attacker could exploit this vulnerability by sending a crafted, heavy stream of SNMP traffic to the targeted device. An exploit could allow the attacker to cause the device to reload unexpectedly, causing a DoS condition. Cisco Bug IDs: CSCvg22135. **CVE ID : CVE-2018-0209**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-550x	O-CIS-SMALL-20418/262
Staros					
Execute Code	08-03-2018	7.2	A vulnerability in the CLI of the Cisco StarOS operating system for Cisco ASR 5000 Series Aggregation Services Routers could allow an authenticated, local attacker to execute arbitrary commands with root privileges on an affected operating system. The vulnerability is	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-	O-CIS-STARO-20418/263

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			due to insufficient validation of user-supplied input by the affected operating system. An attacker could exploit this vulnerability by authenticating to an affected system and injecting malicious arguments into a vulnerable CLI command. A successful exploit could allow the attacker to execute arbitrary commands with root privileges on the affected system. Cisco Bug IDs: CSCvg38807. **CVE ID : CVE-2018-0224**	20180307-staros1	
Citrix					
Netscaler Application Delivery Controller Firmware;Netscaler Gateway Firmware					
XSS	06-03-2018	4.3	Multiple cross-site scripting (XSS) vulnerabilities in Citrix NetScaler ADC 10.5, 11.0, 11.1, and 12.0, and NetScaler Gateway 10.5, 11.0, 11.1, and 12.0 allow remote attackers to inject arbitrary web script or HTML via the Citrix NetScaler interface. **CVE ID : CVE-2018-6811**	https://support.citrix.com/article/CTX232161	O-CIT-NETSC-20418/264
Directory Traversal	06-03-2018	5	Directory traversal vulnerability in NetScaler ADC 10.5, 11.0, 11.1, and 12.0, and NetScaler Gateway 10.5, 11.0, 11.1, and 12.0 allows remote attackers to traverse the directory on the target system via a crafted request. **CVE ID : CVE-2018-6810**	https://support.citrix.com/article/CTX232161	O-CIT-NETSC-20418/265
Gain Information	06-03-2018	5	NetScaler ADC 10.5, 11.0, 11.1, and 12.0, and NetScaler Gateway 10.5, 11.0, 11.1, and 12.0 allow remote attackers to download arbitrary files on the target system. **CVE ID : CVE-2018-6808**	https://support.citrix.com/article/CTX232161	O-CIT-NETSC-20418/266
Gain Privilege	06-03-2018	10	NetScaler ADC 10.5, 11.0, 11.1, and 12.0, and NetScaler Gateway 10.5, 11.0, 11.1, and 12.0 allow remote attackers to gain privilege on a target system. **CVE ID : CVE-2018-6809**	https://support.citrix.com/article/CTX232161	O-CIT-NETSC-20418/267
Corega					
Cg-wgr 1200 Firmware					
Bypass	09-03-2018	5.8	Corega CG-WGR1200 firmware 2.20 and earlier allows an attacker to bypass authentication and change the login password via unspecified vectors.	http://corega.jp/support/security/20180309_w	O-COR-CG-WG-20418/268

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2017-10854	gr1200.htm	
Execute Code Overflow	09-03-2018	8.3	Buffer overflow in Corega CG-WGR1200 firmware 2.20 and earlier allows an attacker to execute arbitrary commands via unspecified vectors. **CVE ID : CVE-2017-10853**	http://corega.jp/support/security/20180309_wgr1200.htm	O-COR-CG-WG-20418/269
Execute Code Overflow	09-03-2018	8.3	Buffer overflow in Corega CG-WGR1200 firmware 2.20 and earlier allows an attacker to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2017-10852**	http://corega.jp/support/security/20180309_wgr1200.htm	O-COR-CG-WG-20418/270
Debian					
Debian Linux					
DoS	09-03-2018	5.1	In libvips before 8.6.3, a NULL function pointer dereference vulnerability was found in the vips_region_generate function in region.c, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted image file. This occurs because of a race condition involving a failed delayed load and other worker threads. **CVE ID : CVE-2018-7998**	NA	O-DEB-DEBIA-20418/271
NA	05-03-2018	6.8	HTTPRedirect.php in the saml2 library in SimpleSAMLphp before 1.15.4 has an incorrect check of return values in the signature validation utilities, allowing an attacker to get invalid signatures accepted as valid by forcing an error during validation. This occurs because of a dependency on PHP functionality that interprets a -1 error code as a true boolean value. **CVE ID : CVE-2018-7711**	https://simplesamlphp.org/security/201803-01	O-DEB-DEBIA-20418/272
D-link					
Dir-860l Firmware;Dir-865l Firmware;Dir-868l Firmware					
XSS	06-03-2018	4.3	XSS vulnerability in htdocs/webinc/js/bsc_sms_inbox.php in D-Link DIR-868L DIR868LA1_FW112b04 and previous versions, DIR-865L DIR-865L_REVA_FIRMWARE_PATCH_1.08.B01 and previous versions, and DIR-860L DIR860LA1_FW110b04 and previous	ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DIR-868L/REVA/DIR-	O-D-L-DIR-8-20418/273

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			versions allows remote attackers to read a cookie via a crafted Treturn parameter to soap.cgi. **CVE ID : CVE-2018-6529**	868L_REVA_FIRMWARE_PATCH_NOTES_1.20B01_EN_WW.pdf	
XSS	06-03-2018	4.3	XSS vulnerability in htdocs/webinc/body/bsc_sms_send.php in D-Link DIR-868L DIR868LA1_FW112b04 and previous versions, DIR-865L DIR-865L_REVA_FIRMWARE_PATCH_1.08.B01 and previous versions, and DIR-860L DIR860LA1_FW110b04 and previous versions allows remote attackers to read a cookie via a crafted receiver parameter to soap.cgi. **CVE ID : CVE-2018-6528**	ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DIR-868L/REVA/DIR-868L_REVA_FIRMWARE_PATCH_NOTES_1.20B01_EN_WW.pdf	O-D-L-DIR-8-20418/274
XSS	06-03-2018	4.3	XSS vulnerability in htdocs/webinc/js/adv_parent_ctrl_map.php in D-Link DIR-868L DIR868LA1_FW112b04 and previous versions, DIR-865L DIR-865L_REVA_FIRMWARE_PATCH_1.08.B01 and previous versions, and DIR-860L DIR860LA1_FW110b04 and previous versions allows remote attackers to read a cookie via a crafted deviceid parameter to soap.cgi.**CVE ID : CVE-2018-6527**	ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DIR-860L/REVA/DIR-860L_REVA_FIRMWARE_PATCH_NOTES_1.11B01_EN_WW.pdf	O-D-L-DIR-8-20418/275
Execute Code	06-03-2018	10	OS command injection vulnerability in soap.cgi (soapcgi_main in cgibin) in D-Link DIR-880L DIR-880L_REVA_FIRMWARE_PATCH_1.08B04 and previous versions, DIR-868L DIR868LA1_FW112b04 and previous versions, DIR-65L DIR-865L_REVA_FIRMWARE_PATCH_1.08.B01 and previous versions, and DIR-860L DIR860LA1_FW110b04 and previous versions allows remote attackers to execute arbitrary OS commands via the service parameter. **CVE ID : CVE-2018-6530**	ftp://FTP2.DLINK.COM/SECURITY_ADVISEMENTS/DIR-868L/REVA/DIR-868L_REVA_FIRMWARE_PATCH_NOTES_1.20B01_EN_WW.pdf	O-D-L-DIR-8-20418/276
Draytek					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
Ap910c Firmware					
XSS	06-03-2018	4.3	Cross-site scripting (XSS) vulnerability in DrayTek Vigor AP910C devices with firmware 1.2.0_RC3 build r6594 allows remote attackers to inject arbitrary web script or HTML via vectors involving home.asp. **CVE ID : CVE-2017-11650**	https://iscouncil.blogspot.in/2018/03/dray-tek-vigor-ap910c-multiple.html	O-DRA-AP910-20418/277
Cross-Site Request Forgery	06-03-2018	6.8	Cross-site request forgery (CSRF) vulnerability in DrayTek Vigor AP910C devices with firmware 1.2.0_RC3 build r6594 allows remote attackers to hijack the authentication of unspecified users for requests that enable SNMP on the remote device via vectors involving goform/setSnmp. **CVE ID : CVE-2017-11649**	https://iscouncil.blogspot.in/2018/03/dray-tek-vigor-ap910c-multiple.html	O-DRA-AP910-20418/278
Emerson					
Controlwave Micro Firmware					
Overflow	07-03-2018	5	A Stack-based Buffer Overflow issue was discovered in Emerson Process Management ControlWave Micro Process Automation Controller: ControlWave Micro [ProConOS v.4.01.280] firmware: CWM v.05.78.00 and prior. A stack-based buffer overflow vulnerability caused by sending crafted packets on Port 20547 could force the PLC to change its state into halt mode. **CVE ID : CVE-2018-5452**	NA	O-EME-CONTR-20418/279
Fedoraproject					
Fedora					
NA	08-03-2018	4.6	Simple Desktop Display Manager (SDDM) before 0.10.0 allows local users to log in as user "sddm" without authentication. **CVE ID : CVE-2014-7271**	https://github.com/sddm/sddm/wiki/0.10.0-Release-Announcement	O-FED-FEDOR-20418/280
DoS Bypass	06-03-2018	6.5	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos	https://bugs.debian.org/cgi-	O-FED-FEDOR-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module. **CVE ID : CVE-2018-5729**	bin/bugreport.cgi?bug=891869	281
Gain Privileges	08-03-2018	7.2	Simple Desktop Display Manager (SDDM) before 0.10.0 allows local users to gain root privileges because code running as root performs write operations within a user home directory, and this user may have created links in advance (exploitation requires the user to win a race condition in the ~/.Xauthority chown case, but not other cases). **CVE ID : CVE-2014-7272**	https://github.com/sddm/sddm/pull/280	O-FED-FEDOR-20418/282
Freebsd					
Freebsd					
NA	09-03-2018	9	In FreeBSD before 11.1-STABLE, 11.1-RELEASE-p7, 10.4-STABLE, 10.4-RELEASE-p7, and 10.3-RELEASE-p28, the kernel does not properly validate IPsec packets coming from a trusted host. Additionally, a use-after-free vulnerability exists in the IPsec AH handling code. This issue could cause a system crash or other unpredictable results.**CVE ID : CVE-2018-6916**	NA	O-FRE-FREEB-20418/283
Google					
Android					
Gain Information	06-03-2018	5	NVIDIA driver contains a possible out-of-bounds read vulnerability due to a leak which may lead to information disclosure. This issue is rated as moderate. Android: A-63851980. **CVE ID : CVE-2017-6280**	https://source.android.com/security/bulletin/pixel/2017-12-01	O-GOO-ANDRO-20418/284
Chrome Os					
Execute Code Overflow	06-03-2018	10	Chrome OS before 53.0.2785.144 allows remote attackers to execute arbitrary commands at boot. **CVE ID : CVE-2016-5179**	https://bugs.chromium.org/p/chromium/issues/detail?id=649039	O-GOO-CHROM-20418/285
Google;Nvidia					

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Android/Shield Tv Firmware					
DoS	06-03-2018	3.6	NVIDIA TrustZone Software contains a vulnerability in the Keymaster implementation where the software reads data past the end, or before the beginning, of the intended buffer; and may lead to denial of service or information disclosure. This issue is rated as high. **CVE ID : CVE-2017-6295**	http://nvidia.custhelp.com/app/answers/detail/a_id/4631	O-GOO-ANDRO-20418/286
DoS	06-03-2018	4.4	NVIDIA TrustZone Software contains a TOCTOU issue in the DRM application which may lead to the denial of service or possible escalation of privileges. This issue is rated as moderate. **CVE ID : CVE-2017-6296**	http://nvidia.custhelp.com/app/answers/detail/a_id/4631	O-GOO-ANDRO-20418/287
+Info	06-03-2018	4.9	NVIDIA Security Engine contains a vulnerability in the RSA function where the keyslot read/write lock permissions are cleared on a chip reset which may lead to information disclosure. This issue is rated as high.**CVE ID : CVE-2017-6283**	http://nvidia.custhelp.com/app/answers/detail/a_id/4631	O-GOO-ANDRO-20418/288
NA	06-03-2018	7.2	NVIDIA Tegra kernel driver contains a vulnerability in NVMAP where an attacker has the ability to write an arbitrary value to an arbitrary location which may lead to an escalation of privileges. This issue is rated as high. **CVE ID : CVE-2017-6282**	http://nvidia.custhelp.com/app/answers/detail/a_id/4631	O-GOO-ANDRO-20418/289
Huawei					
Ar120-s Firmware;Ar1200 Firmware;Ar1200-s Firmware;Ar150 Firmware;Ar150-s Firmware;Ar160 Firmware;Ar200 Firmware;Ar200-s Firmware;Ar2200-s Firmware;Ar3200 Firmware;Ar510 Firmware;Netengine16ex Firmware;S12700 Firmware;S2700 Firmware;S5700 Firmware;S6700 Firmware;S7700 Firmware;S9700 Firmware;Srg1300 Firmware;Srg2300 Firmware;Srg3300 Firmware					
Execute Code	09-03-2018	7.1	Huawei AR120-S V200R005C32; AR1200 V200R005C32; AR1200-S V200R005C32; AR150 V200R005C32; AR150-S V200R005C32; AR160 V200R005C32; AR200 V200R005C32; AR200-S V200R005C32; AR2200-S V200R005C32; AR3200 V200R005C32; V200R007C00; AR510 V200R005C32; NetEngine16EX V200R005C32; SRG1300 V200R005C32; SRG2300 V200R005C32; SRG3300	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180214-01-ospf-en	O-HUA-AR120-20418/290

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			V200R005C32 have an out-of-bounds write vulnerability. When a user executes a query command after the device received an abnormal OSPF message, the software writes data past the end of the intended buffer due to the insufficient verification of the input data. An unauthenticated, remote attacker could exploit this vulnerability by sending abnormal OSPF messages to the device. A successful exploit could cause the system to crash. **CVE ID : CVE-2017-17250**		
Cloudengine 12800 Firmware					
NA	09-03-2018	3.3	Huawei CloudEngine 12800 V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00 have a memory leak vulnerability. An unauthenticated attacker may send specific Label Distribution Protocol (LDP) packets to the devices. When the values of some parameters in the packet are abnormal, the LDP processing module does not release the memory to handle the packet, resulting in memory leak. **CVE ID : CVE-2016-8784**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161221-01-ldp-en	O-HUA-CLOUD-20418/291
Cloudengine 12800 Firmware					
NA	09-03-2018	5	Huawei CloudEngine 12800 V100R003C00, V100R003C10, V100R005C00, V100R005C10, V100R006C00 have a memory leak vulnerability. An unauthenticated attacker may send specific Label Distribution Protocol (LDP) packets to the devices repeatedly. Due to improper validation of some specific fields of the packet, the LDP processing module does not release the memory, resulting in memory leak.**CVE ID : CVE-2016-8782**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161214-01-ldp-en	O-HUA-CLOUD-20418/292
Dp300 Firmware					
NA	09-03-2018	4.9	Huawei DP300 V500R002C00 have a DoS vulnerability due to the lack of validation when the malloc is called. An	http://www.huawei.com/en/psirt/se	O-HUA-DP300-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			authenticated local attacker can craft specific XML files to the affected products and parse this file, which result in DoS attacks. **CVE ID : CVE-2017-17148**	curity-advisories/huawei-sa-20171215-01-xml-en	293
Overflow	09-03-2018	4.9	Huawei DP300 V500R002C00 have an integer overflow vulnerability due to the lack of validation. An authenticated local attacker can craft specific XML files to the affected products and parse this file, which result in DoS attacks. **CVE ID : CVE-2017-17147**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171215-01-xml-en	O-HUA-DP300-20418/294
NA	09-03-2018	5.5	The CIDAM Protocol on Huawei DP300 V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00B012; V500R002C00B013; V500R002C00B014; V500R002C00B017; V500R002C00B018; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00 has an input validation vulnerability due to insufficient validation of specific messages when the protocol is implemented. An authenticated remote attacker could send a malicious message to a target system. Successful exploit could allow the attacker to tamper with business and make the system abnormal. **CVE ID : CVE-2017-17304**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171220-02-cidam-en	O-HUA-DP300-20418/295
NA	09-03-2018	5.5	The CIDAM Protocol on Huawei DP300 V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00B012; V500R002C00B013; V500R002C00B014; V500R002C00B017; V500R002C00B018; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171220-02-cidam-en	O-HUA-DP300-20418/296

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00 has an input validation vulnerability due to insufficient validation of specific messages when the protocol is implemented. An authenticated remote attacker could send a malicious message to a target system. Successful exploit could allow the attacker to tamper with business and make the system abnormal. **CVE ID : CVE-2017-17170**		
NA	09-03-2018	5.5	The CIDAM Protocol on Huawei DP300 V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00B012; V500R002C00B013; V500R002C00B014; V500R002C00B017; V500R002C00B018; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00 has an input validation vulnerability due to insufficient validation of specific messages when the protocol is implemented. An authenticated remote attacker could send a malicious message to a target system. Successful exploit could allow the attacker to tamper with business and make the system abnormal. **CVE ID : CVE-2017-17169**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171220-02-cidam-en	O-HUA-DP300-20418/297
NA	09-03-2018	5.5	The CIDAM Protocol on Huawei DP300 V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00B012; V500R002C00B013; V500R002C00B014; V500R002C00B017; V500R002C00B018; V500R002C00SPC100;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-DP300-20418/298

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00 has an input validation vulnerability due to insufficient validation of specific messages when the protocol is implemented. An authenticated remote attacker could send a malicious message to a target system. Successful exploit could allow the attacker to tamper with business and make the system abnormal. **CVE ID : CVE-2017-17168**	20171220-02-cidam-en	
Execute Code Overflow	09-03-2018	7.2	Huawei DP300 V500R002C00 have a buffer overflow vulnerability due to the lack of validation. An authenticated local attacker can craft specific XML files to the affected products and parse this file, which result in DoS attacks or remote code execution on the device. **CVE ID : CVE-2017-17146**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171215-01-xml-en	O-HUA-DP300-20418/299
Dp300 Firmware;Ecns210 Td Firmware;Espace U1981 Firmware;Nip6600 Firmware;Secospace Usg6500 Firmware;Te60 Firmware;Tp3106 Firmware;Viewpoint 8660 Firmware;Viewpoint 9030 Firmware;Vp9660 Firmware					
DoS	09-03-2018	4.9	Huawei DP300 V500R002C00, NIP6600 V500R001C00, V500R001C20, V500R001C30, Secospace USG6500 V500R001C00, V500R001C20, V500R001C30, TE60 V100R001C01, V100R001C10, V100R003C00, V500R002C00, V600R006C00, TP3106 V100R001C06, V100R002C00, VP9660 V200R001C02, V200R001C30, V500R002C00, V500R002C10, ViewPoint 8660 V100R008C03, ViewPoint 9030 V100R011C02, V100R011C03, eCNS210_TD V100R004C10, eSpace U1981 V200R003C30 have a DoS vulnerability caused by memory exhaustion in some Huawei products. For	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171201-01-pse-en	O-HUA-DP300-20418/300

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			lacking of adequate input validation, attackers can craft and send some malformed messages to the target device to exhaust the memory of the device and cause a Denial of Service (DoS). **CVE ID : CVE-2017-15323**		
Dp300 Firmware;Espace U1960 Firmware;Espace U1981 Firmware;Rp200 Firmware;Rse6500 Firmware;Te30 Firmware;Te40 Firmware;Te50 Firmware;Te60 Firmware;Tp3106 Firmware;Tp3206 Firmware;Viewpoint 9030 Firmware					
Overflow	05-03-2018	5	Backup feature of SIP module in Huawei DP300 V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; RP200 V500R002C00SPC200; V600R006C00; V600R006C00SPC200; RSE6500 V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC300T; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00T; TE30 V100R001C10; V100R001C10SPC100; V100R001C10SPC200B010; V100R001C10SPC300; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700B010; V100R001C10SPC800; V500R002C00SPC200; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; TE40 V500R002C00SPC600;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171206-01-sip-en	O-HUA-DP300-20418/301

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE50 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE60 V100R001C01SPC100; V100R001C01SPC107TB010; V100R001C10; V100R001C10SPC300; V100R001C10SPC400; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700; V100R001C10SPC800; V100R001C10SPC900; V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; V500R002C00SPCb00; V500R002C00SPCd00; V600R006C00; V600R006C00SPC100; V600R006C00SPC200; V600R006C00SPC300; TP3106 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C00SPC800; TP3206 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C10; ViewPoint 9030 V100R011C02SPC100; V100R011C03B012SP15; V100R011C03B012SP16; V100R011C03B015SP03; V100R011C03LGWL01SPC100;		

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			V100R011C03SPC100; V100R011C03SPC200; V100R011C03SPC300; V100R011C03SPC400; V100R011C03SPC500; eSpace U1960 V200R003C30SPC200; eSpace U1981 V100R001C20SPC700; V200R003C20SPCa00 has an overflow vulnerability when the module process a specific amount of state. The module cannot handle it causing SIP module DoS. **CVE ID : CVE-2017-17144**		
Overflow	05-03-2018	5	SIP module in Huawei DP300 V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; RP200 V500R002C00SPC200; V600R006C00; V600R006C00SPC200; RSE6500 V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC300T; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00T; TE30 V100R001C10; V100R001C10SPC100; V100R001C10SPC200B010; V100R001C10SPC300; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700B010; V100R001C10SPC800; V500R002C00SPC200; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171206-01-sip-en	O-HUA-DP300-20418/302

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			V500R002C00SPCb00; V600R006C00; TE40 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE50 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE60 V100R001C01SPC100; V100R001C01SPC107TB010; V100R001C10; V100R001C10SPC300; V100R001C10SPC400; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700; V100R001C10SPC800; V100R001C10SPC900; V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; V500R002C00SPCb00; V500R002C00SPCd00; V600R006C00; V600R006C00SPC100; V600R006C00SPC200; V600R006C00SPC300; TP3106 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C00SPC800; TP3206 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C10; ViewPoint 9030 V100R011C02SPC100; V100R011C03B012SP15; V100R011C03B012SP16;		

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			V100R011C03B015SP03; V100R011C03LGWL01SPC100; V100R011C03SPC100; V100R011C03SPC200; V100R011C03SPC300; V100R011C03SPC400; V100R011C03SPC500; eSpace U1960 V200R003C30SPC200; eSpace U1981 V100R001C20SPC700; V200R003C20SPCa00 has an overflow vulnerability that the module cannot parse a malformed SIP message when validating variables. Attacker can exploit it to make one process reboot at random. **CVE ID : CVE-2017-17143**		
Overflow	05-03-2018	5	SIP module in Huawei DP300 V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; RP200 V500R002C00SPC200; V600R006C00; V600R006C00SPC200; RSE6500 V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC300T; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00T; TE30 V100R001C10; V100R001C10SPC100; V100R001C10SPC200B010; V100R001C10SPC300; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700B010; V100R001C10SPC800; V500R002C00SPC200; V500R002C00SPC500;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171206-01-sip-en	O-HUA-DP300-20418/303

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; TE40 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE50 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; TE60 V100R001C01SPC100; V100R001C01SPC107TB010; V100R001C10; V100R001C10SPC300; V100R001C10SPC400; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700; V100R001C10SPC800; V100R001C10SPC900; V500R002C00; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; V500R002C00SPCb00; V500R002C00SPCd00; V600R006C00; V600R006C00SPC100; V600R006C00SPC200; V600R006C00SPC300; TP3106 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C00SPC800; TP3206 V100R002C00; V100R002C00SPC200; V100R002C00SPC400; V100R002C00SPC600; V100R002C00SPC700; V100R002C10;		

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			ViewPoint 9030 V100R011C02SPC100; V100R011C03B012SP15; V100R011C03B012SP16; V100R011C03B015SP03; V100R011C03LGWL01SPC100; V100R011C03SPC100; V100R011C03SPC200; V100R011C03SPC300; V100R011C03SPC400; V100R011C03SPC500; eSpace U1960 V200R003C30SPC200; eSpace U1981 V100R001C20SPC700; V200R003C20SPCa00 has an overflow vulnerability that attacker can exploit by sending a specially crafted SIP message leading to a process reboot at random. **CVE ID : CVE-2017-17142**		
Dp300 Firmware;Rp200 Firmware;Te30 Firmware;Te40 Firmware;Te50 Firmware;Te60 Firmware					
Gain Information	09-03-2018	4	Huawei DP300 V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00B012; V500R002C00B013; V500R002C00B014; V500R002C00B017; V500R002C00B018; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC400; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; RP200 V500R002C00SPC200; V600R006C00; V600R006C00SPC200; V600R006C00SPC300; TE30 V100R001C10SPC300; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700B010; V500R002C00SPC200; V500R002C00SPC500; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171220-01-cidam-en	O-HUA-DP300-20418/304

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; V600R006C00SPC300; TE40 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC900; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; V600R006C00SPC300; TE50 V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPCb00; V600R006C00; V600R006C00SPC200; V600R006C00SPC300; TE60 V100R001C10; V100R001C10B001; V100R001C10B002; V100R001C10B010; V100R001C10B011; V100R001C10B012; V100R001C10B013; V100R001C10B014; V100R001C10B016; V100R001C10B017; V100R001C10B018; V100R001C10B019; V100R001C10SPC400; V100R001C10SPC500; V100R001C10SPC600; V100R001C10SPC700; V100R001C10SPC800B011; V100R001C10SPC900; V500R002C00; V500R002C00B010; V500R002C00B011; V500R002C00SPC100; V500R002C00SPC200; V500R002C00SPC300; V500R002C00SPC600; V500R002C00SPC700; V500R002C00SPC800; V500R002C00SPC900; V500R002C00SPCa00; V500R002C00SPCb00; V500R002C00SPCd00; V500R002C00SPCe00; V600R006C00; V600R006C00SPC100; V600R006C00SPC200; V600R006C00SPC300 use the CIDAM protocol, which contains sensitive information in the message when it is implemented. So these products has an		

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			information disclosure vulnerability. An authenticated remote attacker could track and get the message of a target system. Successful exploit could allow the attacker to get the information and cause the sensitive information disclosure. **CVE ID : CVE-2017-17303**		
Gain Information	09-03-2018	4	SFTP module in Huawei DP300 V500R002C00; RP200 V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 has an out-of-bounds read vulnerability. A remote, authenticated attacker could exploit this vulnerability by sending specially crafted messages to a target device. Successful exploit may cause some information leak. **CVE ID : CVE-2017-17281**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180228-01-sftp-en	O-HUA-DP300-20418/305
NA	09-03-2018	4.3	Media Gateway Control Protocol (MGCP) in Huawei DP300 V500R002C00; RP200 V500R002C00SPC200; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 has an out-of-bounds write vulnerability. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may impact availability of product service. **CVE ID : CVE-2017-17217**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180124-01-mgcp-en	O-HUA-DP300-20418/306
NA	09-03-2018	4.3	Media Gateway Control Protocol (MGCP) in Huawei DP300 V500R002C00; RP200 V500R002C00SPC200; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 have an	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180124-01-mgcp-en	O-HUA-DP300-20418/307

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			out-of-bounds read vulnerability. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may cause process reboot. **CVE ID : CVE-2017-17216**		
NA	09-03-2018	4.3	Huawei DP300 V500R002C00; RP200 V500R002C00; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 have an out-of-bounds read vulnerability due to the improper processing of malformed H323 messages. A remote attacker that controls a server could exploit this vulnerability by sending malformed H323 reply messages to a target device. Successful exploit could make the device read out of bounds and probably make a service unavailable. **CVE ID : CVE-2017-17200**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180207-03-h323-en	O-HUA-DP300-20418/308
NA	09-03-2018	4.3	Huawei DP300 V500R002C00; RP200 V500R002C00; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 have an out-of-bounds read vulnerability due to the improper processing of malformed H323 messages. A remote attacker that controls a server could exploit this vulnerability by sending malformed H323 reply messages to a target device. Successful exploit could make the device read out of bounds and probably make a service unavailable. **CVE ID : CVE-2017-17199**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180207-03-h323-en	O-HUA-DP300-20418/309
NA	09-03-2018	5	SCCPX module in Huawei DP300 V500R002C00; RP200 V500R002C00;	http://www.huawei.com	O-HUA-DP300-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 has an invalid memory access vulnerabilities. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may impact availability of product service. **CVE ID : CVE-2017-17220**	/en/psirt/security-advisories/huawei-sa-20180207-01-sccpx-en	20418/ 310
NA	09-03-2018	5	SCCPX module in Huawei DP300 V500R002C00; RP200 V500R002C00; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 has an invalid memory access vulnerabilities. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may impact availability of product service. **CVE ID : CVE-2017-17219**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180207-01-sccpx-en	O-HUA-DP300-20418/ 311
NA	09-03-2018	5	SCCPX module in Huawei DP300 V500R002C00; RP200 V500R002C00; V600R006C00; TE30 V100R001C10; V500R002C00; V600R006C00; TE40 V500R002C00; V600R006C00; TE50 V500R002C00; V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00 has an out-of-bounds read vulnerability. An unauthenticated, remote attacker crafts malformed packets with specific parameter to the affected products. Due to insufficient validation of packets, successful exploitation may impact availability of product service.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180207-01-sccpx-en	O-HUA-DP300-20418/ 312

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			CVE ID : CVE-2017-17218		
NA	05-03-2018	6.3	Huawei DP300 V500R002C00; RP200 V500R002C00; V600R006C00; TE30 V100R001C10; V600R006C00; TE50 V600R006C00; TE60 V100R001C10; V500R002C00; V600R006C00; VP9660 V500R002C10 have an DoS vulnerability due to insufficient validation of the parameter when a putty comment key is loaded. An authenticated remote attacker can place a malformed putty key file in system when a system manager load the key an infinite loop happens which lead to reboot the system. **CVE ID : CVE-2017-17131**	http://www.huawei.com/en/psirt/security-advisories/2017/huawei-sa-20171206-01-vpp-en	O-HUA-DP300-20418/313
Dp300 Firmware;Tp3206 Firmware;Viewpoint 9030 Firmware					
NA	09-03-2018	4.3	Huawei DP300 V500R002C00; TP3206 V100R002C00; ViewPoint 9030 V100R011C02; V100R011C03 have a use of a broken or risky cryptographic algorithm vulnerability. The software uses risky cryptographic algorithm in SSL. This is dangerous because a remote unauthenticated attacker could use well-known techniques to break the algorithm. Successful exploit could result in the exposure of sensitive information. **CVE ID : CVE-2017-17167**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171215-01-ssl-en	O-HUA-DP300-20418/314
Espace 7910 Firmware;Espace 7950 Firmware;Espace 8950 Firmware					
Directory Traversal Gain Information	09-03-2018	8	Huawei eSpace 7910 V200R003C30; eSpace 7950 V200R003C30; eSpace 8950 V200R003C00; V200R003C30 have a directory traversal vulnerability. An authenticated, remote attacker can craft specific URL to the affected products. Due to insufficient verification of the URL, successful exploit will upload and download files and cause information leak and system crash. **CVE ID : CVE-2017-17223**	http://www.huawei.com/en/psirt/security-advisories/2018/huawei-sa-20180131-02-espace-en	O-HUA-ESPAC-20418/315
Espace 7950 Firmware;Espace 8950 Firmware					
Execute Code	09-03-2018	6.5	Import Language Package function in Huawei eSpace 7950 V200R003C30;	http://www.huawei.com	O-HUA-ESPAC-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			eSpace 8950 V200R003C00; V200R003C30 has a remote code execution vulnerability. An authenticated, remote attacker can craft and send the packets to the affected products after Language Package is uploaded. Due to insufficient verification of the packets, this could be exploited to execute arbitrary code. **CVE ID : CVE-2017-17222**	/en/psirt/security-advisories/2018/huawei-sa-20180131-01-espace-en	20418/ 316
Execute Code	09-03-2018	6.5	Import Signal Tone function in Huawei eSpace 7950 V200R003C30; eSpace 8950 V200R003C00; V200R003C30 has a remote code execution vulnerability. An authenticated, remote attacker can craft and send the packets to the affected products after the Signal Tone is uploaded. Due to insufficient verification of the packets, this could be exploited to execute arbitrary code. **CVE ID : CVE-2017-17221**	http://www.huawei.com/en/psirt/security-advisories/2018/huawei-sa-20180131-01-espace-en	O-HUA-ESPAC-20418/ 317
Eva-al10 Firmware;Eva-cl00 Firmware;Eva-dl00 Firmware;Eva-l09 Firmware;Eva-l19 Firmware;Eva-l29 Firmware;Eva-tl00 Firmware;Vie-l09 Firmware;Vie-l29 Firmware					
DoS	05-03-2018	4.3	Some Huawei smart phones with software EVA-L09C34B142; EVA-L09C40B196; EVA-L09C432B210; EVA-L09C440B138; EVA-L09C464B150; EVA-L09C530B127; EVA-L09C55B190; EVA-L09C576B150; EVA-L09C635B221; EVA-L09C636B193; EVA-L09C675B130; EVA-L09C688B143; EVA-L09C703B160; EVA-L09C706B145; EVA-L09GBRC555B171; EVA-L09IRLC368B160; EVA-L19C10B190; EVA-L19C185B220; EVA-L19C20B160; EVA-L19C432B210; EVA-L19C636B190; EVA-L29C20B160; EVA-L29C636B191; EVA-TL00C01B198; VIE-L09C02B131; VIE-L09C109B181; VIE-L09C113B170; VIE-L09C150B170; VIE-L09C25B120; VIE-L09C40B181; VIE-L09C432B181; VIE-L09C55B170; VIE-L09C605B131; VIE-L09ITAC555B130; VIE-L29C10B170; VIE-L29C185B181; VIE-L29C605B131; VIE-L29C636B202	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171129-01-smartphone-en	O-HUA-EVA-A-20418/ 318

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			have a denial of service (DoS) vulnerability. An attacker can trick a user to install a malicious application to exploit this vulnerability. Successful exploitation can cause camera application unusable. **CVE ID : CVE-2017-8164**		
Hicinema					
Gain Information	09-03-2018	4.3	Huawei video applications HiCinema with software of 8.0.3.308; 8.0.4.300 have a permission control vulnerability. Due to improper verification of specific interface, an attacker who is on the same network with the user can obtain some information through a man-in-the-middle attack.**CVE ID : CVE-2017-17325**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180307-01-hicinema-en	O-HUA-HICIN-20418/319
Honor 6 Firmware					
Overflow	09-03-2018	9.3	Touchscreen drive in Huawei H60 (Honor 6) Versions earlier than H60-L02_6.12.16 and P9 Plus Versions earlier than VIE-AL10BC00B356 has a stack overflow vulnerabilities. An attacker tricks a user into installing a malicious application on the smart phone, and send given parameter to touchscreen drive to crash the system or escalate privilege. **CVE ID : CVE-2016-8783**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161215-01-smartphone-en	O-HUA-HONOR-20418/320
Honor Smart Scale Application Firmware					
Gain Information	09-03-2018	4.3	Huawei Honor Smart Scale Application with software of 1.1.1 has an information disclosure vulnerability. The application does not sufficiently restrict the resource which can be accessed by certain protocol. An attacker could trick the user to click a malicious link, successful exploit could cause information disclosure. **CVE ID : CVE-2017-17322**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180309-01-ah-en	O-HUA-HONOR-20418/321
Ibmc Firmware					
NA	09-03-2018	4	Huawei iBMC V200R002C10; V200R002C20; V200R002C30 have an improper authorization vulnerability. The software incorrectly performs an	http://www.huawei.com/en/psirt/security-	O-HUA-IBMC -20418/322

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
			authorization check when a normal user attempts to access certain information which is supposed to be accessed only by admin user. Successful exploit could cause information disclosure. **CVE ID : CVE-2017-17323**	advisories/2018/huawei-sa-20180131-01-ibmc-en	
Mate 9 Pro Firmware					
Execute Code Overflow	09-03-2018	6.8	Huawei Mate 9 Pro smartphones with software LON-AL00BC00B139D; LON-AL00BC00B229 have an integer overflow vulnerability. The camera driver does not validate the external input parameters and causes an integer overflow, which in the after processing results in a buffer overflow. An attacker tricks the user to install a crafted application, successful exploit could cause malicious code execution. **CVE ID : CVE-2017-17324**	http://www.huawei.com/en/psirt/security-advisories/2018/huawei-sa-20180124-01-smartphone-en	O-HUA-MATE -20418/323
Mha-al00a Firmware					
NA	09-03-2018	4.3	Huawei smartphones with software of MHA-AL00AC00B125 have an improper resource management vulnerability. The software does not properly manage the resource when do device register operation. An attacker tricks the user who has root privilege to install a crafted application, successful exploit could cause certain service unavailable. **CVE ID : CVE-2017-17327**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171220-03-smartphone-en	O-HUA-MHA-A-20418/324
Overflow	09-03-2018	7.1	Huawei smartphones with software of MHA-AL00AC00B125 have an integer overflow vulnerability. The software does not process certain variable properly when handle certain process. An attacker tricks the user who has root privilege to install a crafted application, successful exploit could cause information disclosure. **CVE ID : CVE-2017-17328**	http://www.huawei.com/en/psirt/security-advisories/2017/huawei-sa-20171220-01-smartphone-en	O-HUA-MHA-A-20418/325
Nip6300 Firmware;Nip6600 Firmware;Secospace Usg6300 Firmware;Secospace Usg6500 Firmware					
Execute Code	09-03-2018	6.8	Patch module of Huawei NIP6300 V500R001C20SPC100,	http://www.huawei.com	O-HUA-NIP63-

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			V500R001C20SPC200, NIP6600 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6300 V500R001C20SPC100, V500R001C20SPC200, Secospace USG6500 V500R001C20SPC100, V500R001C20SPC200 has a memory leak vulnerability. An authenticated attacker could execute special commands many times, the memory leaking happened, which would cause the device to reset finally. **CVE ID : CVE-2017-15315**	/en/psirt/security-advisories/huawei-sa-20171129-01-command-en	20418/326
S12700 Firmware;S1700 Firmware;S2700 Firmware;S3700 Firmware;S5700 Firmware;S6700 Firmware;S7700 Firmware;S9700 Firmware					
NA	05-03-2018	4.3	Huawei S12700 V200R005C00; V200R006C00; V200R007C00; V200R007C01; V200R007C20; V200R008C00; V200R009C00;S1700 V200R006C10; V200R009C00;S2700 V100R006C03; V200R003C00; V200R005C00; V200R006C00; V200R006C10; V200R007C00; V200R007C00B050; V200R007C00SPC009T; V200R007C00SPC019T; V200R008C00; V200R009C00;S3700 V100R006C03;S5700 V200R001C00; V200R001C01; V200R002C00; V200R003C00; V200R003C02; V200R005C00; V200R005C01; V200R005C02; V200R005C03; V200R006C00; V200R007C00; V200R008C00; V200R009C00;S6700 V200R001C00; V200R001C01; V200R002C00; V200R003C00; V200R005C00; V200R005C01; V200R005C02; V200R008C00; V200R009C00;S7700 V200R001C00; V200R001C01; V200R002C00; V200R003C00; V200R005C00; V200R006C00; V200R006C01; V200R007C00; V200R007C01; V200R008C00; V200R008C06; V200R009C00;S9700 V200R001C00;	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20171206-01-mpls-en	O-HUA-S1270-20418/327

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			V200R001C01; V200R002C00; V200R003C00; V200R005C00; V200R006C00; V200R007C00; V200R007C01; V200R008C00; V200R009C00 have a memory leak vulnerability. In some specific conditions, if attackers send specific malformed MPLS Service PING messages to the affected products, products do not release the memory when handling the packets. So successful exploit will result in memory leak of the affected products. **CVE ID : CVE-2017-17141**		
S12700 Firmware;S5700 Firmware;S6700 Firmware;S7700 Firmware;S9700 Firmware					
DoS Overflow	09-03-2018	7.8	Huawei S12700 V200R005C00, V200R006C00, V200R007C00, V200R008C00, S5700 V200R006C00, V200R007C00, V200R008C00, S6700 V200R008C00, S7700 V200R001C00, V200R002C00, V200R003C00, V200R005C00, V200R006C00, V200R007C00, V200R008C00, S9700 V200R001C00, V200R002C00, V200R003C00, V200R005C00, V200R006C00, V200R007C00, V200R008C00 have a denial of service (DoS) vulnerability. Due to the lack of input validation, a remote attacker may craft a malformed Resource Reservation Protocol (RSVP) packet and send it to the device, causing a few buffer overflows and occasional device restart. **CVE ID : CVE-2016-8786**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161228-01-rsvp-en	O-HUA-S1270-20418/328
S12700 Firmware;S5700 Firmware;S7700 Firmware;S9700 Firmware					
Gain Information	09-03-2018	4.3	Huawei S12700 V200R007C00, V200R008C00, S5700 V200R007C00, S7700 V200R002C00, V200R005C00, V200R006C00, V200R007C00, V200R008C00, S9700 V200R007C00 have an input validation vulnerability. Due to the lack of input validation, an attacker may craft a malformed packet and send it to the device using VRP,	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20161228-04-vrp-en	O-HUA-S1270-20418/329

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			causing the device to display additional memory data and possibly leading to sensitive information leakage. **CVE ID : CVE-2016-8785**		
Industrial.softing					
Fg-100 Pb Profibus Firmware					
NA	09-03-2018	10	Softing FG-100 PB PROFIBUS firmware version FG-x00-PB_V2.02.0.00 contains a hardcoded password for the root account, which allows remote attackers to obtain administrative access via a TELNET session. **CVE ID : CVE-2014-6617**		O-IND-FG-10-20418/ 330
Linux					
Linux Kernel					
DoS Overflow Memory Corruption	08-03-2018	4.6	In the Linux kernel before 4.12, Hisilicon Network Subsystem (HNS) does not consider the ETH_SS_PRIV_FLAGS case when retrieving sset_count data, which allows local users to cause a denial of service (buffer overflow and memory corruption) or possibly have unspecified other impact, as demonstrated by incompatibility between hns_get_sset_count and ethtool_get_strings. **CVE ID : CVE-2017-18222**	NA	O-LIN-LINUX-20418/ 331
Linux Kernel					
DoS	02-03-2018	4.7	The netfilter subsystem in the Linux kernel through 4.15.7 mishandles the case of a rule blob that contains a jump but lacks a user-defined chain, which allows local users to cause a denial of service (NULL pointer dereference) by leveraging the CAP_NET_RAW or CAP_NET_ADMIN capability, related to arpt_do_table in net/ipv4/netfilter/arp_tables.c, ipt_do_table in net/ipv4/netfilter/ip_tables.c, and ip6t_do_table in net/ipv6/netfilter/ip6_tables.c. **CVE ID : CVE-2018-1065**	NA	O-LIN-LINUX-20418/ 332
DoS	09-03-2018	4.7	** DISPUTED ** Race condition in the	NA	O-LIN-

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			store_int_with_restart() function in arch/x86/kernel/cpu/mcheck/mce.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (panic) by leveraging root access to write to the check_interval file in a /sys/devices/system/machinecheck/machinecheck<cpu number> directory. NOTE: a third party has indicated that this report is not security relevant. **CVE ID : CVE-2018-7995**		LINUX-20418/333
DoS	01-03-2018	4.9	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping. **CVE ID : CVE-2017-18208**	NA	O-LIN-LINUX-20418/334
DoS Overflow	07-03-2018	4.9	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (BUG) via a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages system call. **CVE ID : CVE-2018-7740**	https://bugzilla.kernel.org/show_bug.cgi?id=199037	O-LIN-LINUX-20418/335
DoS	07-03-2018	4.9	The __munlock_pagevec function in mm/mlock.c in the Linux kernel before 4.11.4 allows local users to cause a denial of service (NR_MLOCK accounting corruption) via crafted use of mlockall and munlockall system calls. **CVE ID : CVE-2017-18221**	NA	O-LIN-LINUX-20418/336
Bypass Gain Information	08-03-2018	5	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR. **CVE ID : CVE-2018-7755**	https://lkml.org/lkml/2018/3/7/1116	O-LIN-LINUX-20418/337

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
NA	02-03-2018	7.1	The Linux kernel before version 4.11 is vulnerable to a NULL pointer dereference in fs/cifs/cifsencrypt.c:setup_ntlmv2_rsp() that allows an attacker controlling a CIFS server to kernel panic a client that has this server mounted, because an empty TargetInfo field in an NTLMSSP setup negotiation response is mishandled during session recovery. **CVE ID : CVE-2018-1066**	NA	O-LIN-LINUX-20418/ 338
DoS	05-03-2018	7.2	In drivers/net/ethernet/hisilicon/ hns/ hns_enet.c in the Linux kernel before 4.13, local users can cause a denial of service (use-after-free and BUG) or possibly have unspecified other impact by leveraging differences in skb handling between hns_nic_net_xmit_hw and hns_nic_net_xmit. **CVE ID : CVE-2017-18218**	NA	O-LIN-LINUX-20418/ 339
Moxa					
Oncell G3110-hspa Firmware;Oncell G3110-hspa-t Firmware;Oncell G3150-hspa Firmware;Oncell G3150-hspa-t Firmware					
DoS	05-03-2018	3.3	A NULL Pointer Dereference issue was discovered in Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior. The application does not check for a NULL value, allowing for an attacker to perform a denial of service attack. **CVE ID : CVE-2018-5449**	https://ics-cert.us-cert.gov/advisories/ICSA-18-060-02	O-MOX-ONCEL-20418/ 340
Bypass	05-03-2018	7.5	A Reliance on Cookies without Validation and Integrity Checking issue was discovered in Moxa OnCell G3100-HSPA Series version 1.4 Build 16062919 and prior. The application allows a cookie parameter to consist of only digits, allowing an attacker to perform a brute force attack bypassing authentication and gaining access to device functions. **CVE ID : CVE-2018-5455**	https://ics-cert.us-cert.gov/advisories/ICSA-18-060-02	O-MOX-ONCEL-20418/ 341
NA	05-03-2018	7.8	An Improper Handling of Length Parameter Inconsistency issue was discovered in Moxa OnCell G3100-HSPA	https://ics-cert.us-cert.gov/adv	O-MOX-ONCEL-20418/

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			Series version 1.4 Build 16062919 and prior. An attacker may be able to edit the element of an HTTP request, causing the device to become unavailable. **CVE ID : CVE-2018-5453**	isories/ICSA-18-060-02	342
Opensuse					
Leap					
NA	01-03-2018	9	The packaging of NextCloud in openSUSE used /srv/www/htdocs in an unsafe manner, which could have allowed scripts running as wwwrun user to escalate privileges to root during nextcloud package upgrade. **CVE ID : CVE-2017-9286**	https://www.suse.com/de-de/security/CVE ID : CVE/CVE ID : CVE-2017-9286/	O-OPE-LEAP-20418/343
Opensuse;Suse					
Leap/Linux Enterprise Software Development Kit					
NA	01-03-2018	5	The build package before 20171128 did not check directory names during extraction of build results that allowed untrusted builds to write outside of the target system,allowing escape out of buildroots. **CVE ID : CVE-2017-14804**	NA	O-OPE-LEAP/-20418/344
Polycom					
Qdx 6000 Firmware					
XSS	07-03-2018	4.3	Stored XSS exists on Polycom QDX 6000 devices. **CVE ID : CVE-2018-7564**	https://support.polycom.com/content/dam/polycom-support/global/documentation/security-advisory-vulnerabilities-qdx-6000-1-0.pdf	O-POL-QDX 6-20418/345
Cross-Site Request Forgery	07-03-2018	6.8	CSRF exists on Polycom QDX 6000 devices. **CVE ID : CVE-2018-7565**	https://support.polycom.com/content/dam/po	O-POL-QDX 6-20418/346

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
				lycom-support/global/documentation/security-advisory-vulnerabilities-qdx-6000-1-0.pdf	
Redhat					
Enterprise Linux;Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Workstation					
DoS Overflow	01-03-2018	5	A stack buffer overflow flaw was found in the way 389-ds-base 1.3.6.x before 1.3.6.13, 1.3.7.x before 1.3.7.9, 1.4.x before 1.4.0.5 handled certain LDAP search filters. A remote, unauthenticated attacker could potentially use this flaw to make ns-slapd crash via a specially crafted LDAP request, thus resulting in denial of service. **CVE ID : CVE-2017-15134**	https://bugzilla.redhat.com/show_bug.cgi?id=1531573	O-RED-ENTER-20418/347
Siemens					
En100 Ethernet Module Dnp3 Firmware;En100 Ethernet Module Iec 104 Firmware;En100 Ethernet Module Modbus Tcp Firmware;En100 Ethernet Module Profinet Io Firmware					
NA	08-03-2018	3.5	A vulnerability has been identified in Siemens DIGSI 4 (All versions < V4.92), EN100 Ethernet module IEC 61850 variant (All versions < V4.30), EN100 Ethernet module PROFINET IO variant (All versions), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module DNP3 variant (All versions), EN100 Ethernet module IEC 104 variant (All versions), SIPROTEC Compact 7SJ80 (All versions < V4.77), SIPROTEC Compact 7SK80 (All versions < V4.77), SIPROTEC Compact 7SJ66 (All versions < V4.30), Other SIPROTEC Compact relays (All versions), Other SIPROTEC 4 relays (All versions). An attacker with local access to the engineering system or in a privileged	https://cert-portal.siemens.com/productcert/pdf/ssa-203306.pdf	O-SIE-EN100-20418/348

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			network position and able to obtain certain network traffic could possibly reconstruct access authorization passwords. **CVE ID : CVE-2018-4839**		
NA	08-03-2018	5	A vulnerability has been identified in Siemens DIGSI 4 (All versions < V4.92), EN100 Ethernet module IEC 61850 variant (All versions < V4.30), EN100 Ethernet module PROFINET IO variant (All versions), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module DNP3 variant (All versions), EN100 Ethernet module IEC 104 variant (All versions). The device engineering mechanism allows an unauthenticated remote user to upload a modified device configuration overwriting access authorization passwords. **CVE ID : CVE-2018-4840**	https://cert-portal.siemens.com/productcert/pdf/ssa-203306.pdf	O-SIE-EN100-20418/349
NA	08-03-2018	5	A vulnerability has been identified in Siemens EN100 Ethernet module IEC 61850 variant (All versions < V4.30), EN100 Ethernet module PROFINET IO variant (All versions), EN100 Ethernet module Modbus TCP variant (All versions), EN100 Ethernet module DNP3 variant (All versions), EN100 Ethernet module IEC 104 variant (All versions). The web interface (TCP/80) of affected devices allows an unauthenticated user to upgrade or downgrade the firmware of the device, including to older versions with known vulnerabilities. **CVE ID : CVE-2018-4838**	https://cert-portal.siemens.com/productcert/pdf/ssa-845879.pdf	O-SIE-EN100-20418/350
Sowifi					
Connect So Wifi Hotspot Firmware					
NA	07-03-2018	5.8	Open redirect vulnerability in the SO Connect SO WIFI hotspot web interface, prior to version 140, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL. **CVE ID : CVE-2018-7473**	https://blog.redyops.com/CVE ID : CVE-2018-7473-open-url-redirection-	O-SOW-CONNE-20418/351

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
				vulnerability/	
Tendacn					
Ac9 Firmware					
DoS Overflow	01-03-2018	7.5	Stack-based Buffer Overflow in httpd on Tenda AC9 devices V15.03.05.14_EN allows remote attackers to cause a denial of service or possibly have unspecified other impact. **CVE ID : CVE-2018-7561**	https://github.com/VulDetailsPublication/Poc/tree/master/Tenda/AC9	O-TEN-AC9 F-20418/352
Operating System ; Application (OS;Application)					
Canonical/Memcached					
Ubuntu Linux/Memcached					
DoS	05-03-2018	5	Memcached version 1.5.5 contains an Insufficient Control of Network Message Volume (Network Amplification, CWE-406) vulnerability in the UDP support of the memcached server that can result in denial of service via network flood (traffic amplification of 1:50,000 has been reported by reliable sources). This attack appear to be exploitable via network connectivity to port 11211 UDP. This vulnerability appears to have been fixed in 1.5.6 due to the disabling of the UDP protocol by default. **CVE ID : CVE-2018-1000115**	https://www.synology.com/support/security/Synology_SA_18_07	O-CAN-UBUNT-20418/353
Canonical;Debian/Djangoproject					
Ubuntu Linux/Debian Linux/Django					
NA	09-03-2018	5	An issue was discovered in Django 2.0 before 2.0.3, 1.11 before 1.11.11, and 1.8 before 1.8.19. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable. **CVE ID : CVE-2018-7537**	https://www.djangoproject.com/weblog/2018/mar/06/security-releases/	O-CAN-UBUNT-20418/354

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
NA	09-03-2018	5	An issue was discovered in Django 2.0 before 2.0.3, 1.11 before 1.11.11, and 1.8 before 1.8.19. The django.utils.html.urlize() function was extremely slow to evaluate certain inputs due to catastrophic backtracking vulnerabilities in two regular expressions (only one regular expression for Django 1.8.x). The urlize() function is used to implement the urlize and urlizetrunc template filters, which were thus vulnerable. **CVE ID : CVE-2018-7536**	https://www.djangoproject.com/weblog/2018/mar/06/security-releases/	O-CAN-UBUNT-20418/355
Canonical;Debian/Dovecot					
Ubuntu Linux/Debian Linux/Dovecot					
DoS	02-03-2018	4.3	A denial of service flaw was found in dovecot before 2.2.34. An attacker able to generate random SNI server names could exploit TLS SNI configuration lookups, leading to excessive memory usage and the process to restart. **CVE ID : CVE-2017-15130**	https://bugzilla.redhat.com/show_bug.cgi?id=1532356	O-CAN-UBUNT-20418/356
Debian/Drupal					
Debian Linux/Drupal					
Bypass	01-03-2018	3.5	Drupal core 7.x versions before 7.57 when using Drupal's private file system, Drupal will check to make sure a user has access to a file before allowing the user to view or download it. This check fails under certain conditions in which one module is trying to grant access to the file and another is trying to deny it, leading to an access bypass vulnerability. This vulnerability is mitigated by the fact that it only occurs for unusual site configurations. **CVE ID : CVE-2017-6928**	NA	O-DEB-DEBIA-20418/357
XSS	01-03-2018	4.3	A jQuery cross site scripting vulnerability is present when making Ajax requests to untrusted domains. This vulnerability is mitigated by the fact that it requires contributed or custom modules in order to exploit. For Drupal 8, this vulnerability was already fixed in Drupal 8.4.0 in the Drupal core upgrade to jQuery 3. For	NA	O-DEB-DEBIA-20418/358

CV Scoring Scale (CVSS)	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	Reference/ Patch	NCIIPC ID
			Drupal 7, it is fixed in the current release (Drupal 7.57) for jQuery 1.4.4 (the version that ships with Drupal 7 core) as well as for other newer versions of jQuery that might be used on the site, for example using the jQuery Update module. **CVE ID : CVE-2017-6929**		
XSS	01-03-2018	4.3	Drupal 8.4.x versions before 8.4.5 and Drupal 7.x versions before 7.57 has a Drupal.checkPlain() JavaScript function which is used to escape potentially dangerous text before outputting it to HTML (as JavaScript output does not typically go through Twig autoescaping). This function does not correctly handle all methods of injecting malicious HTML, leading to a cross-site scripting vulnerability under certain circumstances. The PHP functions which Drupal provides for HTML escaping are not affected. **CVE ID : CVE-2017-6927**	NA	O-DEB-DEBIA-20418/ 359
NA	01-03-2018	5.8	Drupal core 7.x versions before 7.57 has an external link injection vulnerability when the language switcher block is used. A similar vulnerability exists in various custom and contributed modules. This vulnerability could allow an attacker to trick users into unwillingly navigating to an external site. **CVE ID : CVE-2017-6932**	NA	O-DEB-DEBIA-20418/ 360
Debian/Libming					
Debian Linux/Libming					
DoS Overflow	08-03-2018	4.3	There is a heap-based buffer overflow in the getString function of util/decompile.c in libming 0.4.8 for DOUBLE data. A Crafted input will lead to a denial of service attack. **CVE ID : CVE-2018-7877**	NA	O-DEB-DEBIA-20418/ 361
DoS	08-03-2018	4.3	In libming 0.4.8, a memory exhaustion vulnerability was found in the function parseSWF_ACTIONRECORD in util/parser.c, which allows remote attackers to cause a denial of service via a crafted file. **CVE ID : CVE-2018-7876**	NA	O-DEB-DEBIA-20418/ 362

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Reference/ Patch	NCIIPC ID
DoS Overflow	08-03-2018	4.3	There is a heap-based buffer over-read in the getString function of util/decompile.c in libming 0.4.8 for CONSTANT8 data. A Crafted input will lead to a denial of service attack. **CVE ID : CVE-2018-7875**	NA	O-DEB-DEBIA-20418/ 363
DoS Overflow	08-03-2018	4.3	An invalid memory address dereference was discovered in strlenext in util/decompile.c in libming 0.4.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-7874**	NA	O-DEB-DEBIA-20418/ 364
DoS Overflow	08-03-2018	4.3	There is a heap-based buffer overflow in the getString function of util/decompile.c in libming 0.4.8 for INTEGER data. A Crafted input will lead to a denial of service attack.**CVE ID : CVE-2018-7873**	NA	O-DEB-DEBIA-20418/ 365
DoS Overflow	08-03-2018	4.3	An invalid memory address dereference was discovered in the function getName in libming 0.4.8 for CONSTANT16 data. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-7872**	NA	O-DEB-DEBIA-20418/ 366
DoS Overflow	08-03-2018	4.3	An invalid memory address dereference was discovered in getString in util/decompile.c in libming 0.4.8 for CONSTANT16 data. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-7870**	NA	O-DEB-DEBIA-20418/ 367
DoS	08-03-2018	4.3	There is a memory leak triggered in the function dcinit of util/decompile.c in libming 0.4.8, which will lead to a denial of service attack. **CVE ID : CVE-2018-7869**	NA	O-DEB-DEBIA-20418/ 368
DoS Overflow	08-03-2018	4.3	There is a heap-based buffer over-read in the getName function of util/decompile.c in libming 0.4.8 for CONSTANT8 data. A Crafted input will lead to a denial of service attack. **CVE ID : CVE-2018-7868**	NA	O-DEB-DEBIA-20418/ 369
DoS Overflow	08-03-2018	4.3	There is a heap-based buffer overflow in the getString function of util/decompile.c in libming 0.4.8 during a RegisterNumber	NA	O-DEB-DEBIA-20418/

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
			sprintf. A Crafted input will lead to a denial of service attack. **CVE ID : CVE-2018-7867**		370
DoS	08-03-2018	4.3	A NULL pointer dereference was discovered in newVar3 in util/decompile.c in libming 0.4.8. The vulnerability causes a segmentation fault and application crash, which leads to denial of service. **CVE ID : CVE-2018-7866**	NA	O-DEB-DEBIA-20418/ 371
DoS Overflow	08-03-2018	6.8	There is a heap-based buffer over-read in the getName function of util/decompile.c in libming 0.4.8 for CONSTANT16 data. A crafted input will lead to a denial of service or possibly unspecified other impact.**CVE ID : CVE-2018-7871**	NA	O-DEB-DEBIA-20418/ 372
Debian/Net-snmp					
Debian Linux/Net-snmp					
Execute Code Overflow	07-03-2018	7.5	NET-SNMP version 5.7.2 contains a heap corruption vulnerability in the UDP protocol handler that can result in command execution. **CVE ID : CVE-2018-1000116**	https://sourceforge.net/p/net-snmp/bugs/2821/	O-DEB-DEBIA-20418/ 373
Debian;Redhat/Jasper Project					
Debian Linux/Enterprise Linux Desktop;Enterprise Linux Server;Enterprise Linux Server Eus;Enterprise Linux Workstation/Jasper					
NA	09-03-2018	4.3	JasPer before version 2.0.12 is vulnerable to a use-after-free in the way it decodes certain JPEG 2000 image files resulting in a crash on the application using JasPer. **CVE ID : CVE-2016-9591**	https://bugzilla.redhat.com/show_bug.cgi?id=1406405	O-DEB-DEBIA-20418/ 374
Debian;Ubuntu/Dovecot					
Debian Linux/Ubuntu/Dovecot					
DoS	02-03-2018	5.5	A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server. **CVE ID : CVE-2017-14461**	NA	O-DEB-DEBIA-20418/ 375
Fedoraproject/MIT					

CV Scoring Scale (CVSS)	**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	Reference/ Patch	NCIIPC ID
Fedora/Kerberos					
NA	06-03-2018	5.5	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN. **CVE ID : CVE-2018-5730**	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=891869	O-FED-FEDOR-20418/376
Freebsd/NTP					
Freebsd/NTP					
Execute Code Overflow	08-03-2018	7.5	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array. **CVE ID : CVE-2018-7183**	http://support.ntp.org/bin/view/Main/NtpBug3414	O-FRE-FREEB-20418/377
Opensuse/Xv Project					
Leap/XV					
Execute Code Memory Corruption	05-03-2018	7.5	xvpng.c in xv 3.10a has memory corruption (out-of-bounds write) when decoding PNG comment fields, leading to crashes or potentially code execution, because it uses an incorrect length value. **CVE ID : CVE-2017-18215**	NA	O-OPE-LEAP/-20418/378
Redhat/Selinux Project					
Enterprise Linux/Selinux					
NA	02-03-2018	3.3	Context relabeling of filesystems is vulnerable to symbolic link attack, allowing a local, unprivileged malicious entity to change the SELinux context of an arbitrary file to a context with few restrictions. This only happens when the relabeling process is done, usually when taking SELinux state from disabled to enable (permissive or enforcing). The issue was found in policycoreutils 2.5-11. **CVE ID : CVE-2018-1063**	https://bugzilla.redhat.com/show_bug.cgi?id=1550122	O-RED-ENTER-20418/379

CV Scoring Scale (CVSS)	**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;							