



National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

16 Feb - 28 Feb 2019

Vol. 06 No. 04

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
advancename					
advancecomp					
N/A	27-02-2019	4.3	In AdvanceCOMP 2.1, png_compress in pngex.cc in advpng has an integer overflow upon encountering an invalid PNG size, which results in an attempted memcpy to write into a buffer that is too small. (There is also a heap-based buffer over-read.) CVE ID : CVE-2019-9210	N/A	A-ADV-ADVA-030419/1
antfin					
sofa-hessian					
N/A	27-02-2019	7.5	SOFA-Hessian through 4.0.2 allows remote attackers to execute arbitrary commands via a crafted serialized Hessian object because blacklisting of com.caucho.naming.QName and com.sun.org.apache.xpath.internal.objects.XString is mishandled, related to Resin Gadget. CVE ID : CVE-2019-9212	N/A	A-ANT-SOFA-030419/2
Appneta					
Tcpreplay					
N/A	16-02-2019	6.8	An issue was discovered in Tcpreplay 4.3.1. A NULL pointer	N/A	A-APP-TCPR-030419/3

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dereference occurred in the function <code>get_layer4_v6()</code> located at <code>get.c</code> . This can be triggered by sending a crafted pcap file to the <code>tcpreplay-edit</code> binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8376		
N/A	16-02-2019	6.8	An issue was discovered in Tcpreplay 4.3.1. A NULL pointer dereference occurred in the function <code>get_ipv6_l4proto()</code> located at <code>get.c</code> . This can be triggered by sending a crafted pcap file to the <code>tcpreplay-edit</code> binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8377	N/A	A-APP-TCPR-030419/4
N/A	16-02-2019	6.8	An issue was discovered in Tcpreplay 4.3.1. An invalid memory access occurs in <code>do_checksum</code> in <code>checksum.c</code> . It can be triggered by sending a crafted pcap file to the <code>tcpreplay-edit</code> binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8381	N/A	A-APP-TCPR-030419/5
ascellamobile					
musicloud					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	16-02-2019	4.8	A file-read vulnerability was identified in the Wi-Fi transfer feature of Musiccloud 1.6. By default, the application runs a transfer service on port 8080, accessible by everyone on the same Wi-Fi network. An attacker can send the POST parameters downfiles and cur-folder (with a crafted ../payload) to the download.script endpoint. This will create a MusicPlayerArchive.zip archive that is publicly accessible and includes the content of any requested file (such as the /etc/passwd file). CVE ID : CVE-2019-8389	N/A	A-ASC-MUSI-030419/6
auction_website_script_project					
auction_website_script					
N/A	23-02-2019	4	PHP Scripts Mall Auction website script 2.0.4 allows parameter tampering of the payment amount. CVE ID : CVE-2019-9063	N/A	A-AUC-AUCT-030419/7
Avaya					
one-x_communicator					
N/A	26-02-2019	2.1	Avaya one-X Communicator uses weak cryptographic algorithms in the client authentication component that could allow a local attacker to decrypt sensitive information. Affected versions include all 6.2.x versions prior to 6.2 SP13.	https://downloads.avaya.com/css/P8/documents/101055661	A-AVA-ONE--030419/8

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-7006		
axiosys					
bento4					
N/A	16-02-2019	6.8	An issue was discovered in Bento4 1.5.1-628. A heap-based buffer over-read exists in AP4_BitStream::ReadBytes() in Codecs/Ap4BitStream.cpp, a similar issue to CVE-2017-14645. It can be triggered by sending a crafted file to the aac2mp4 binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8378	N/A	A-AXI-BENT-030419/9
N/A	16-02-2019	6.8	An issue was discovered in Bento4 1.5.1-628. A NULL pointer dereference occurs in AP4_Track::GetSampleIndexForTimeStampMs() located in Core/Ap4Track.cpp. It can be triggered by sending a crafted file to the mp4audioclip binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8380	N/A	A-AXI-BENT-030419/10
N/A	16-02-2019	6.8	An issue was discovered in Bento4 1.5.1-628. A NULL pointer dereference occurs in the function AP4_List::Find located in Core/Ap4List.h when called from Core/Ap4Movie.cpp.	N/A	A-AXI-BENT-030419/11

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			It can be triggered by sending a crafted file to the mp4dump binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-8382							
b3log										
symphony										
N/A	25-02-2019	4.3	An issue was discovered in b3log Symphony (aka Sym) before v3.4.7. XSS exists via the userIntro and userNickname fields to processor/SettingsProcessor.java. CVE ID : CVE-2019-9142	N/A	A-B3L-SYMP-030419/12					
bagesoft										
bagecms										
N/A	17-02-2019	6.5	upload/protected/modules/admini/views/post/index.php in BageCMS through 3.1.4 allows SQL Injection via the title or titleAlias parameter. CVE ID : CVE-2019-8421	N/A	A-BAG-BAGE-030419/13					
baigo										
baigo_cms										
N/A	28-02-2019	4.3	An issue was discovered in baigo CMS 2.1.1. There is a persistent XSS vulnerability that allows remote attackers to inject arbitrary web script or HTML via the opt[base][BG_SITE_NAME] parameter to the	N/A	A-BAI-BAIG-030419/14					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bg_console/index.php?m=opt&c=request URL. CVE ID : CVE-2019-9226		
N/A	28-02-2019	7.5	An issue was discovered in baigo CMS 2.1.1. There is a vulnerability that allows remote attackers to execute arbitrary code. A BG_SITE_NAME parameter with malicious code can be written into the opt_base.inc.php file. CVE ID : CVE-2019-9227	N/A	A-BAI-BAIG-030419/15
bosch					
smart_camera					
N/A	22-02-2019	5.1	An issue was discovered in the Bosch Smart Camera App before 1.3.1 for Android. Due to improperly implemented TLS certificate checks, a malicious actor could potentially succeed in executing a man-in-the-middle attack for some connections. (The Bosch Smart Home App is not affected. iOS Apps are not affected.) CVE ID : CVE-2019-7728	https://psirt.bosch.com/Advisory/BO-SCH-2019-0202.html	A-BOS-SMAR-030419/16
N/A	22-02-2019	2.1	An issue was discovered in the Bosch Smart Camera App before 1.3.1 for Android. Due to setting of insecure permissions, a malicious app could potentially succeed in retrieving video clips or still images that have been cached for clip sharing. (The Bosch Smart Home App is not affected. iOS Apps are not	https://psirt.bosch.com/Advisory/BO-SCH-2019-0204.html	A-BOS-SMAR-030419/17

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected.) CVE ID : CVE-2019-7729		
british_airways					
entertainment_system					
N/A	22-02-2019	4.6	The British Airways Entertainment System, as installed on Boeing 777-36N(ER) and possibly other aircraft, does not prevent the USB charging/data-transfer feature from interacting with USB keyboard and mouse devices, which allows physically proximate attackers to conduct unanticipated attacks against Entertainment applications, as demonstrated by using mouse copy-and-paste actions to trigger a Chat buffer overflow or possibly have unspecified other impact. CVE ID : CVE-2019-9019	N/A	A-BRI-ENTE-030419/18
CA					
privileged_access_manager					
N/A	26-02-2019	6.4	An improper authentication vulnerability in CA Privileged Access Manager 3.x Web-UI jk-manager and jk-status allows a remote attacker to gain sensitive information or alter configuration. CVE ID : CVE-2019-7392	N/A	A-CA-PRIV-030419/19
cab_booking_script_project					
cab_booking_script					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	23-02-2019	5	PHP Scripts Mall Cab Booking Script 1.0.3 allows Directory Traversal into the parent directory of a jpg or png file. CVE ID : CVE-2019-9064	N/A	A-CAB-CAB_-030419/20

Cisco

webex_meetings_online

N/A	28-02-2019	9	A vulnerability in the update service of Cisco Webex Meetings Desktop App and Cisco Webex Productivity Tools for Windows could allow an authenticated, local attacker to execute arbitrary commands as a privileged user. The vulnerability is due to insufficient validation of user-supplied parameters. An attacker could exploit this vulnerability by invoking the update service command with a crafted argument. An exploit could allow the attacker to run arbitrary commands with SYSTEM user privileges. While the CVSS Attack Vector metric denotes the requirement for an attacker to have local access, administrators should be aware that in Active Directory deployments, the vulnerability could be exploited remotely by leveraging the operating system remote management tools. This vulnerability is fixed in Cisco Webex Meetings Desktop App Release 33.6.6 and 33.9.1	N/A	A-CIS-WEBE-030419/21
-----	------------	---	---	-----	----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			releases. This vulnerability is fixed in Cisco Webex Productivity Tools Release 33.0.7. CVE ID : CVE-2019-1674		

prime_infrastructure

N/A	21-02-2019	5.8	A vulnerability in the Identity Services Engine (ISE) integration feature of Cisco Prime Infrastructure (PI) could allow an unauthenticated, remote attacker to perform a man-in-the-middle attack against the Secure Sockets Layer (SSL) tunnel established between ISE and PI. The vulnerability is due to improper validation of the server SSL certificate when establishing the SSL tunnel with ISE. An attacker could exploit this vulnerability by using a crafted SSL certificate and could then intercept communications between the ISE and PI. A successful exploit could allow the attacker to view and alter potentially sensitive information that the ISE maintains about clients that are connected to the network. This vulnerability affects Cisco Prime Infrastructure Software Releases 2.2 through 3.4.0 when the PI server is integrated with ISE, which is disabled by default. CVE ID : CVE-2019-1659	N/A	A-CIS-PRIM-030419/22
-----	------------	-----	---	-----	----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
prime_collaboration_assurance					
N/A	21-02-2019	6.4	<p>A vulnerability in the Quality of Voice Reporting (QOVR) service of Cisco Prime Collaboration Assurance (PCA) Software could allow an unauthenticated, remote attacker to access the system as a valid user. The vulnerability is due to insufficient authentication controls. An attacker could exploit this vulnerability by connecting to the QOVR service with a valid username. A successful exploit could allow the attacker to perform actions with the privileges of the user that is used for access. This vulnerability affects Cisco PCA Software Releases prior to 12.1 SP2.</p> <p>CVE ID : CVE-2019-1662</p>	N/A	A-CIS-PRIM-030419/23
unity_connection					
N/A	21-02-2019	4.3	<p>A vulnerability in the Security Assertion Markup Language (SAML) single sign-on (SSO) interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the interface of an affected device. An</p>	N/A	A-CIS-UNIT-030419/24

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 affected interface or access sensitive, browser-based information. Version 12.5 is affected. CVE ID : CVE-2019-1685		
cmseasy					
cmseasy					
N/A	17-02-2019	4.3	In CmsEasy 7.0, there is XSS via the ckplayer.php url parameter. CVE ID : CVE-2019-8432	N/A	A-CMS-CMSE-030419/25
N/A	17-02-2019	4.3	In CmsEasy 7.0, there is XSS via the ckplayer.php autoplay parameter. CVE ID : CVE-2019-8434	N/A	A-CMS-CMSE-030419/26
cmswing					
cmswing					
N/A	17-02-2019	5	global.encryptPassword in bootstrap/global.js in CMSWing 1.3.7 relies on multiple MD5 operations for password hashing. CVE ID : CVE-2019-7649	N/A	A-CMS-CMSW-030419/27
cordaware					
bestinformed					
N/A	25-02-2019	4.6	The Scripting and AutoUpdate functionality in Cordaware bestinformed Microsoft Windows client versions before	N/A	A-COR-BEST-030419/28

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.2.1.0 are affected by insecure implementations which allow remote attackers to execute arbitrary commands and escalate privileges. CVE ID : CVE-2019-6265		
N/A	25-02-2019	7.5	Cordaware bestinformed Microsoft Windows client before 6.2.1.0 is affected by insecure SSL certificate verification and insecure access patterns. These issues allow remote attackers to downgrade encrypted connections to cleartext. CVE ID : CVE-2019-6266	N/A	A-COR-BEST-030419/29
custom_t-shirt_ecommerce_script_project					
custom_t-shirt_ecommerce_script					
N/A	23-02-2019	4	PHP Scripts Mall Custom T-Shirt Ecommerce Script 3.1.1 allows parameter tampering of the payment amount. CVE ID : CVE-2019-9065	N/A	A-CUS-CUST-030419/30
Dedecms					
Dedecms					
N/A	16-02-2019	5	DedeCMS through V5.7SP2 allows arbitrary file upload in dede/album_edit.php or dede/album_add.php, as demonstrated by a dede/album_edit.php?dopost=save&formzip=1 request with a ZIP archive that contains a file such as "1.jpg.php" (because input validation only checks	N/A	A-DED-DEDE-030419/31

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			that .jpg, .png, or .gif is present as a substring, and does not otherwise check the file name or content). CVE ID : CVE-2019-8362		
N/A	18-02-2019	6.5	In DedeCMS 5.7SP2, attackers can upload a .php file to the uploads/ directory (without being blocked by the Web Application Firewall), and then execute this file, via this sequence of steps: visiting the management page, clicking on the template, clicking on Default Template Management, clicking on New Template, and modifying the filename from ../index.html to ../index.php. CVE ID : CVE-2019-8933	N/A	A-DED-DEDE-030419/32
deltaww					
screeneditor					
N/A	28-02-2019	4.3	Delta Industrial Automation CNCSoft, CNCSoft ScreenEditor Version 1.00.84 and prior. An out-of-bounds read vulnerability may cause the software to crash due to lacking user input validation for processing project files. CVE ID : CVE-2019-6547	N/A	A-DEL-SCRE-030419/33
Drupal					
Drupal					
N/A	21-02-2019	6.8	Some field types do not properly sanitize data from non-form sources in Drupal 8.5.x	https://www.synology.com/	A-DRU-DRUP-030419/34

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>before 8.5.11 and Drupal 8.6.x before 8.6.10. This can lead to arbitrary PHP code execution in some cases. A site is only affected by this if one of the following conditions is met: The site has the Drupal 8 core RESTful Web Services (rest) module enabled and allows PATCH or POST requests, or the site has another web services module enabled, like JSON:API in Drupal 8, or Services or RESTful Web Services in Drupal 7. (Note: The Drupal 7 Services module itself does not require an update at this time, but you should apply other contributed updates associated with this advisory if Services is in use.)</p> <p>CVE ID : CVE-2019-6340</p>	security/ advisory/ Synology_ SA_19_09	

Eclipse

wakaama

N/A	22-02-2019	5	<p>In Eclipse Wakaama (formerly liblwm2m) 1.0, core/er-coap-13/er-coap-13.c in lwmm2mserver in the LWM2M server mishandles invalid options, leading to a memory leak. Processing of a single crafted packet leads to leaking (wasting) 24 bytes of memory. This can lead to termination of the LWM2M server after exhausting all available memory.</p> <p>CVE ID : CVE-2019-9004</p>	N/A	A-ECL-WAKA-030419/35
-----	------------	---	---	-----	----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
etsi					
enterprise_transport_security					
N/A	26-02-2019	4.3	The ETSI Enterprise Transport Security (ETS, formerly known as eTLS) protocol does not provide per-session forward secrecy. CVE ID : CVE-2019-9191	N/A	A-ETS-ENTE-030419/36
Exiv2					
Exiv2					
N/A	25-02-2019	6.8	An issue was discovered in Exiv2 0.27. There is infinite recursion at Exiv2::Image::printTiffStructure in the file image.cpp. This can be triggered by a crafted file. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9143	N/A	A-EXI-EXIV-030419/37
N/A	25-02-2019	6.8	An issue was discovered in Exiv2 0.27. There is infinite recursion at BigTiffImage::printIFD in the file bigtiffimage.cpp. This can be triggered by a crafted file. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9144	N/A	A-EXI-EXIV-030419/38
F5					
big-ip_access_policy_manager					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/39
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/40
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/41
N/A	26-02-2019	4.3	Cross-site scripting (XSS) vulnerability in F5 BIG-IP Access Policy Manager (APM) 11.5.x and 11.6.x Admin Web UI.	https://support.f5.com/csp/article/K3142492	A-F5-BIG--030419/42

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6595	6	
big-ip_advanced_firewall_manager					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/43
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/44
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/45
big-ip_analytics					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/46
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/47
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/48
big-ip_application_security_manager					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL	https://support.f5.com/csp/	A-F5-BIG--030419/49

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	article/K54167061	
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/50
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/51
big-ip_domain_name_system					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/52

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/53
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/54
big-ip_edge_gateway					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/55
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL	https://support.f5.com/csp/	A-F5-BIG--030419/56

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	article/K10065173	
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/57
big-ip_fraud_protection_service					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/58
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited,	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/59

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593		
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/60
big-ip_global_traffic_manager					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/61
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/62

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593		
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/63

big-ip_link_controller

N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/64
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/65

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593		
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/66

big-ip_local_traffic_manager

N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/67
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.)	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/68

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6593		
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	https://support.f5.com/csp/article/K91026261	A-F5-BIG--030419/69
big-ip_policy_enforcement_manager					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/70
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/71
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/72

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	com/csp/article/K91026261	
big-ip_webaccelerator					
N/A	26-02-2019	6.4	On BIG-IP 14.1.0-14.1.0.1, TMM may restart and produce a core file when validating SSL certificates in client SSL or server SSL profiles. CVE ID : CVE-2019-6592	https://support.f5.com/csp/article/K54167061	A-F5-BIG--030419/73
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.) CVE ID : CVE-2019-6593	https://support.f5.com/csp/article/K10065173	A-F5-BIG--030419/74
N/A	26-02-2019	4.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-13.1.1.1, and 14.0.0-14.0.0.2, Multi-Path TCP (MPTCP) does not protect against multiple	https://support.f5.com/csp/article/K9102626	A-F5-BIG--030419/75

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zero length DATA_FINs in the reassembly queue, which can lead to an infinite loop in some circumstances. CVE ID : CVE-2019-6594	1	
feifeicms					
feifeicms					
N/A	17-02-2019	6.5	FeiFeiCms 4.0.181010 on Windows allows remote attackers to read or delete arbitrary files via index.php?s=Admin-Data-Down-id-..\ or index.php?s=Admin-Data-Del-id-..\ directory traversal. CVE ID : CVE-2019-8412	N/A	A-FEI-FEIF-030419/76
file_project					
file					
N/A	18-02-2019	6.8	do_bid_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printf and file_vprintf. CVE ID : CVE-2019-8904	N/A	A-FIL-FILE-030419/77
N/A	18-02-2019	6.8	do_core_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printable, a different vulnerability than CVE-2018-10360. CVE ID : CVE-2019-8905	N/A	A-FIL-FILE-030419/78
N/A	18-02-2019	6.8	do_core_note in readelf.c in libmagic.a in file 5.35 has an out-of-bounds read because	N/A	A-FIL-FILE-030419/79

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memcpy is misused. CVE ID : CVE-2019-8906		
N/A	18-02-2019	6.8	do_core_note in readelf.c in libmagic.a in file 5.35 allows remote attackers to cause a denial of service (stack corruption and application crash) or possibly have unspecified other impact. CVE ID : CVE-2019-8907	N/A	A-FIL-FILE-030419/80
fizzday					
gorose					
N/A	23-02-2019	7.5	GoRose v1.0.4 has SQL Injection when the order_by or group_by parameter can be controlled. CVE ID : CVE-2019-9047	N/A	A-FIZ-GORO-030419/81
Freedesktop					
Poppler					
N/A	26-02-2019	6.8	A heap-based buffer underwrite exists in ImageStream::getLine() located at Stream.cc in Poppler 0.74.0 that can (for example) be triggered by sending a crafted PDF file to the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9200	N/A	A-FRE-POPP-030419/82
GNU					
Binutils					
N/A	23-02-2019	6.8	An issue was discovered in GNU libiberty, as distributed in GNU	N/A	A-GNU-BINU-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Binutils 2.32. It is a heap-based buffer over-read in d_expression_1 in cp-demangle.c after many recursive calls. CVE ID : CVE-2019-9070		030419/83
N/A	23-02-2019	4.3	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a stack consumption issue in d_count_templates_scopes in cp-demangle.c after many recursive calls. CVE ID : CVE-2019-9071	N/A	A-GNU-BINU-030419/84
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in setup_group in elf.c. CVE ID : CVE-2019-9072	N/A	A-GNU-BINU-030419/85
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in _bfd_elf_slurp_version_tables in elf.c. CVE ID : CVE-2019-9073	N/A	A-GNU-BINU-030419/86
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an out-of-bounds read	N/A	A-GNU-BINU-030419/87

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leading to a SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c. CVE ID : CVE-2019-9074		
N/A	23-02-2019	6.8	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is a heap-based buffer overflow in _bfd_archive_64_bit_slurp_armap in archive64.c. CVE ID : CVE-2019-9075	N/A	A-GNU-BINU-030419/88
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in elf_read_notes in elf.c. CVE ID : CVE-2019-9076	N/A	A-GNU-BINU-030419/89
N/A	23-02-2019	6.8	An issue was discovered in GNU Binutils 2.32. It is a heap-based buffer overflow in process_mips_specific in readelf.c via a malformed MIPS option section. CVE ID : CVE-2019-9077	N/A	A-GNU-BINU-030419/90
pspp					
N/A	27-02-2019	4.3	There is a reachable assertion abort in the function write_long_string_missing_value_s() in data/sys-file-writer.c in libdata.a in GNU PSPP 1.2.0 that	N/A	A-GNU-PSPP-030419/91

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will lead to denial of service. CVE ID : CVE-2019-9211		
Glibc					
N/A	25-02-2019	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match. CVE ID : CVE-2019-9169	N/A	A-GNU-GLIB-030419/92
N/A	26-02-2019	5	** DISPUTED ** In the GNU C Library (aka glibc or libc6) through 2.29, check_dst_limits_calc_pos_1 in posix/regexec.c has Uncontrolled Recursion, as demonstrated by '([])(\\1\\1)*' in grep, a different issue than CVE-2018-20796. NOTE: the software maintainer disputes that this is a vulnerability because the behavior occurs only with a crafted pattern. CVE ID : CVE-2019-9192	N/A	A-GNU-GLIB-030419/93
Google					
Chrome					
N/A	19-02-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy.	N/A	A-GOO-CHRO-030419/94

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5754		
N/A	19-02-2019	5.8	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. CVE ID : CVE-2019-5755	N/A	A-GOO-CHRO-030419/95
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5756	N/A	A-GOO-CHRO-030419/96
N/A	19-02-2019	6.8	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. CVE ID : CVE-2019-5757	N/A	A-GOO-CHRO-030419/97
N/A	19-02-2019	6.8	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5758	N/A	A-GOO-CHRO-030419/98
N/A	19-02-2019	6.8	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a	N/A	A-GOO-CHRO-030419/99

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5759							
N/A	19-02-2019	6.8	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5760	N/A	A-GOO-CHRO-030419/100					
N/A	19-02-2019	6.8	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5761	N/A	A-GOO-CHRO-030419/101					
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5762	N/A	A-GOO-CHRO-030419/102					
N/A	19-02-2019	6.8	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5763	N/A	A-GOO-CHRO-030419/103					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	6.8	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5764	N/A	A-GOO-CHRO-030419/104
N/A	19-02-2019	4.3	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent. CVE ID : CVE-2019-5765	N/A	A-GOO-CHRO-030419/105
N/A	19-02-2019	4.3	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2019-5766	N/A	A-GOO-CHRO-030419/106
N/A	19-02-2019	4.3	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK. CVE ID : CVE-2019-5767	N/A	A-GOO-CHRO-030419/107
N/A	19-02-2019	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome	N/A	A-GOO-CHRO-030419/108

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension. CVE ID : CVE-2019-5768		
N/A	19-02-2019	6.8	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5769	N/A	A-GOO-CHRO-030419/109
N/A	19-02-2019	6.8	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. CVE ID : CVE-2019-5770	N/A	A-GOO-CHRO-030419/110
N/A	19-02-2019	6.8	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2019-5771	N/A	A-GOO-CHRO-030419/111
N/A	19-02-2019	6.8	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.	N/A	A-GOO-CHRO-030419/112

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5772		
N/A	19-02-2019	4.3	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. CVE ID : CVE-2019-5773	N/A	A-GOO-CHRO-030419/113
N/A	19-02-2019	6.8	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file. CVE ID : CVE-2019-5774	N/A	A-GOO-CHRO-030419/114
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5775	N/A	A-GOO-CHRO-030419/115
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5776	N/A	A-GOO-CHRO-030419/116

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5777	N/A	A-GOO-CHRO-030419/117
N/A	19-02-2019	4.3	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. CVE ID : CVE-2019-5778	N/A	A-GOO-CHRO-030419/118
N/A	19-02-2019	4.3	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2019-5779	N/A	A-GOO-CHRO-030419/119
N/A	19-02-2019	4.6	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events. CVE ID : CVE-2019-5780	N/A	A-GOO-CHRO-030419/120
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome	N/A	A-GOO-CHRO-030419/121

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5781		
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2019-5782	N/A	A-GOO-CHRO-030419/122
N/A	19-02-2019	6.8	Missing URI encoding of untrusted input in DevTools in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform a Dangling Markup Injection attack via a crafted HTML page. CVE ID : CVE-2019-5783	N/A	A-GOO-CHRO-030419/123
Hdfgroup					
Hdf5					
N/A	17-02-2019	4.3	A buffer overflow in H5O__layout_encode in H5Olayout.c in the HDF HDF5 through 1.10.4 library allows attackers to cause a denial of service via a crafted HDF5 file. This issue was triggered while repacking an HDF5 file, aka "Invalid write of size 2." CVE ID : CVE-2019-8396	N/A	A-HDF-HDF5-030419/124
N/A	17-02-2019	4.3	An issue was discovered in the HDF HDF5 1.10.4 library. There	N/A	A-HDF-HDF5-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is an out of bounds read in the function H5T_close_real in H5T.c. CVE ID : CVE-2019-8397		030419/125
N/A	17-02-2019	4.3	An issue was discovered in the HDF HDF5 1.10.4 library. There is an out of bounds read in the function H5T_get_size in H5T.c. CVE ID : CVE-2019-8398	N/A	A-HDF-HDF5-030419/126
N/A	25-02-2019	6.8	An issue was discovered in the HDF HDF5 1.10.4 library. There is an out of bounds read in the function H5VM_memcpyvv in H5VM.c when called from H5D_compact_readvv in H5Dcompact.c. CVE ID : CVE-2019-9151	N/A	A-HDF-HDF5-030419/127
N/A	25-02-2019	6.8	An issue was discovered in the HDF HDF5 1.10.4 library. There is an out of bounds read in the function H5MM_xstrdup in H5MM.c when called from H5O_dtype_decode_helper in H5Odtype.c. CVE ID : CVE-2019-9152	N/A	A-HDF-HDF5-030419/128

hongcms_project

hongcms

N/A	17-02-2019	5.5	HongCMS 3.0.0 allows arbitrary file read and write operations via a ../ in the filename parameter to the admin/index.php/language/edit URL. CVE ID : CVE-2019-8407	N/A	A-HON-HONG-030419/129
-----	------------	-----	--	-----	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hornerautomation					
cscape					
N/A	28-02-2019	6.8	Cscape, 9.80 SP4 and prior. An improper input validation vulnerability may be exploited by processing specially crafted POC files. This may allow an attacker to read confidential information and remotely execute arbitrary code. CVE ID : CVE-2019-6555	N/A	A-HOR-CSCA-030419/130
hotels_server_project					
hotels_server					
N/A	17-02-2019	7.5	Hotels_Server through 2018-11-05 has SQL Injection via the API because the controller/api/login.php telephone parameter is mishandled. CVE ID : CVE-2019-8393	N/A	A-HOT-HOTE-030419/131
hsycms					
hsycms					
N/A	25-02-2019	4.3	An issue was discovered in Hsycms V1.1. There is an XSS vulnerability via the name field to the /book page. CVE ID : CVE-2019-9145	N/A	A-HSY-HSYC-030419/132
IBM					
bigfix_platform					
N/A	27-02-2019	5	IBM BigFix Platform 9.2 and 9.5 could allow an attacker to query the relay remotely and gather information about the updates and fixlets deployed to the	N/A	A-IBM-BIGF-030419/133

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			associated sites due to not enabling authenticated access. IBM X-Force ID: 156869. CVE ID : CVE-2019-4061		
idreamsoft					
icms					
N/A	18-02-2019	4.9	An issue was discovered in idreamsoft iCMS through 7.0.14. A CSRF vulnerability can delete users' articles via the public/api.php?app=user URL. CVE ID : CVE-2019-8902	N/A	A-IDR-ICMS-030419/134
indexhibit					
indexhibit					
N/A	20-02-2019	6.5	In Indexhibit 2.1.5, remote attackers can execute arbitrary code via the v parameter (in conjunction with the id parameter) in a upd_jxcode=true action to the ndxzstudio/?a=system URL. CVE ID : CVE-2019-8954	N/A	A-IND-INDE-030419/135
Intel					
unite					
N/A	18-02-2019	7.5	Authentication bypass in the Intel Unite(R) solution versions 3.2 through 3.3 may allow an unauthenticated user to potentially enable escalation of privilege to the Intel Unite(R) Solution administrative portal via network access. CVE ID : CVE-2019-0101	https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00214.ht	A-INT-UNIT-030419/136

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
				ml						
openvino										
N/A	18-02-2019	2.1	Logic error in the installer for Intel(R) OpenVINO(TM) 2018 R3 and before for Linux may allow a privileged user to potentially enable information disclosure via local access. CVE ID : CVE-2019-0127	https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00222.html	A-INT-OPEN-030419/137					
J2store										
J2store										
N/A	26-02-2019	7.5	SQL injection vulnerability in the J2Store plugin 3.x before 3.3.7 for Joomla! allows remote attackers to execute arbitrary SQL commands via the product_option[] parameter. CVE ID : CVE-2019-9184	N/A	A-J2S-J2ST-030419/138					
Jamf										
self_service										
N/A	25-02-2019	7.9	Jamf Self Service 10.9.0 allows man-in-the-middle attackers to obtain a root shell by leveraging the "publish Bash shell scripts" feature to insert "/Applications/Utilities/Terminal app/Contents/MacOS/Terminal" into the TCP data stream. CVE ID : CVE-2019-9146	N/A	A-JAM-SELF-030419/139					
Jenkins										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
script_security					
N/A	20-02-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.52 and earlier in RejectASTTransformsCustomize r.java that allows attackers with Overall/Read permission to provide a Groovy script to an HTTP endpoint that can result in arbitrary code execution on the Jenkins master JVM. CVE ID : CVE-2019-1003024	https://jenkins.io/security/advisory/2019-02-19/#SECURITY-1320	A-JEN-SCRI-030419/140
cloud_foundry					
N/A	20-02-2019	4	A exposure of sensitive information vulnerability exists in Jenkins Cloud Foundry Plugin 2.3.1 and earlier in AbstractCloudFoundryPushDescriptor.java that allows attackers with Overall/Read access to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins. CVE ID : CVE-2019-1003025	https://jenkins.io/security/advisory/2019-02-19/#SECURITY-876	A-JEN-CLOU-030419/141
mattermost					
N/A	20-02-2019	4	A server-side request forgery vulnerability exists in Jenkins Mattermost Notification Plugin 2.6.2 and earlier in MattermostNotifier.java that allows attackers with Overall/Read permission to have Jenkins connect to an	https://jenkins.io/security/advisory/2019-02-19/#SECURITY-985	A-JEN-MATT-030419/142

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker-specified Mattermost server and room and send a message. CVE ID : CVE-2019-1003026		
octopusdeploy					
N/A	20-02-2019	4	A server-side request forgery vulnerability exists in Jenkins OctopusDeploy Plugin 1.8.1 and earlier in OctopusDeployPlugin.java that allows attackers with Overall/Read permission to have Jenkins connect to an attacker-specified URL and obtain the HTTP response code if successful, and exception error message otherwise. CVE ID : CVE-2019-1003027	https://jenkins.io/security/advisory/2019-02-19/#SECURITY-817	A-JEN-OCTO-030419/143
jms_messaging					
N/A	20-02-2019	4	A server-side request forgery vulnerability exists in Jenkins JMS Messaging Plugin 1.1.1 and earlier in SSLCertificateAuthenticationMethod.java, UsernameAuthenticationMethod.java that allows attackers with Overall/Read permission to have Jenkins connect to a JMS endpoint. CVE ID : CVE-2019-1003028	https://jenkins.io/security/advisory/2019-02-19/#SECURITY-1033	A-JEN-JMS_-030419/144
jtbc					
jtbc_php					
N/A	17-02-2019	5	JTBC(PHP) 3.0.1.8 allows Arbitrary File Upload via the	N/A	A-JTB-JTBC-030419/145

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			console/#/console/file/manage.php?type=list URI, as demonstrated by a .php file. CVE ID : CVE-2019-8433		
kohanaframework					
kohana					
N/A	21-02-2019	7.5	Koseven through 3.3.9, and Kohana through 3.3.6, has SQL Injection when the order_by() parameter can be controlled. CVE ID : CVE-2019-8979	N/A	A-KOH-KOHA-030419/146
koseven					
koseven					
N/A	21-02-2019	7.5	Koseven through 3.3.9, and Kohana through 3.3.6, has SQL Injection when the order_by() parameter can be controlled. CVE ID : CVE-2019-8979	N/A	A-KOS-KOSE-030419/147
Laravel					
framework					
N/A	24-02-2019	7.5	The Illuminate component of Laravel Framework 5.7.x has a deserialization vulnerability that can lead to remote code execution if the content is controllable, related to the __destruct method of the PendingCommand class in PendingCommand.php. CVE ID : CVE-2019-9081	N/A	A-LAR-FRAM-030419/148
Libming					
ming					
N/A	24-02-2019	6.8	Ming (aka libming) 0.4.8 has a	N/A	A-LIB-MING-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NULL pointer dereference in the function getString() in the decompile.c file in libutil.a. CVE ID : CVE-2019-9113		030419/149
N/A	24-02-2019	6.8	Ming (aka libming) 0.4.8 has an out of bounds write vulnerability in the function strcpyext() in the decompile.c file in libutil.a. CVE ID : CVE-2019-9114	N/A	A-LIB-MING-030419/150
Live555					
streaming_media					
N/A	27-02-2019	7.5	In Live555 before 2019.02.27, malformed headers lead to invalid memory access in the parseAuthorizationHeader function. CVE ID : CVE-2019-9215	N/A	A-LIV-STRE-030419/151
maccms					
maccms					
N/A	27-02-2019	4.3	Maccms 8.0 allows XSS via the inc/config/cache.php t_key parameter because template/paody/html/vod_type.html mishandles the keywords parameter, and a/tpl/module/db.php only filters the t_name parameter (not t_key). CVE ID : CVE-2019-8410	N/A	A-MAC-MACC-030419/152
matio_project					
matio					
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT	N/A	A-MAT-MATI-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			File I/O Library) 1.5.13. There is a heap-based buffer overflow in the function InflateVarName() in inflate.c when called from ReadNextCell in mat5.c. CVE ID : CVE-2019-9026		030419/153
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a heap-based buffer overflow problem in the function ReadNextCell() in mat5.c. CVE ID : CVE-2019-9027	N/A	A-MAT-MATI-030419/154
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a stack-based buffer over-read in the function InflateDimensions() in inflate.c when called from ReadNextCell in mat5.c. CVE ID : CVE-2019-9028	N/A	A-MAT-MATI-030419/155
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is an out-of-bounds read with a SEGV in the function Mat_VarReadNextInfo5() in mat5.c. CVE ID : CVE-2019-9029	N/A	A-MAT-MATI-030419/156
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a stack-based buffer over-read in Mat_VarReadNextInfo5() in mat5.c.	N/A	A-MAT-MATI-030419/157

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9030		
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a NULL pointer dereference in the function Mat_VarFree() in mat.c. CVE ID : CVE-2019-9031	N/A	A-MAT-MATI-030419/158
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is an out-of-bounds write problem causing a SEGV in the function Mat_VarFree() in mat.c. CVE ID : CVE-2019-9032	N/A	A-MAT-MATI-030419/159
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a stack-based buffer over-read for the "Rank and Dimension" feature in the function ReadNextCell() in mat5.c. CVE ID : CVE-2019-9033	N/A	A-MAT-MATI-030419/160
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a stack-based buffer over-read for a memcpy() in the function ReadNextCell() in mat5.c. CVE ID : CVE-2019-9034	N/A	A-MAT-MATI-030419/161
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a stack-based buffer over-read in the function ReadNextStructField() in	N/A	A-MAT-MATI-030419/162

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mat5.c. CVE ID : CVE-2019-9035		
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a heap-based buffer overflow in the function ReadNextFunctionHandle() in mat5.c. CVE ID : CVE-2019-9036	N/A	A-MAT-MATI-030419/163
N/A	23-02-2019	6.4	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is a buffer over-read in the function Mat_VarPrint() in mat.c. CVE ID : CVE-2019-9037	N/A	A-MAT-MATI-030419/164
N/A	23-02-2019	5	An issue was discovered in libmatio.a in matio (aka MAT File I/O Library) 1.5.13. There is an out-of-bounds read problem with a SEGV in the function ReadNextCell() in mat5.c. CVE ID : CVE-2019-9038	N/A	A-MAT-MATI-030419/165
Mcafee					
endpoint_security					
N/A	28-02-2019	6.1	Privilege Escalation vulnerability in Microsoft Windows client in McAfee Endpoint Security (ENS) 10.6.1 and earlier allows local users to gain elevated privileges via a specific set of circumstances. CVE ID : CVE-2019-3582	https://k.c.mcafee.com/corporate/index?page=content&id=SB10254	A-MCA-ENDP-030419/166

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
Agent											
N/A	28-02-2019	5	Buffer Access with Incorrect Length Value in McAfee Agent (MA) 5.x allows remote unauthenticated users to potentially cause a denial of service via specifically crafted UDP packets. CVE ID : CVE-2019-3598	https://kc.mcafee.com/corporate/index?page=content&id=SB10272	A-MCA-AGEN-030419/167						
N/A	28-02-2019	4.3	Information Disclosure vulnerability in Remote logging (which is disabled by default) in McAfee Agent (MA) 5.x allows remote unauthenticated users to access sensitive information via remote logging when it is enabled. CVE ID : CVE-2019-3599	https://kc.mcafee.com/corporate/index?page=content&id=SB10271	A-MCA-AGEN-030419/168						
Microfocus											
filr											
N/A	20-02-2019	4	A path traversal vulnerability in the web application component of Micro Focus Filr 3.x allows a remote attacker authenticated as a low privilege user to download arbitrary files from the Filr server. This vulnerability affects all versions of Filr 3.x prior to Security Update 6. CVE ID : CVE-2019-3474	N/A	A-MIC-FILR-030419/169						
N/A	20-02-2019	7.2	A local privilege escalation vulnerability in the famtd component of Micro Focus Filr 3.0 allows a local attacker authenticated as a low privilege	N/A	A-MIC-FILR-030419/170						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user to escalate to root. This vulnerability affects all versions of Filr 3.x prior to Security Update 6. CVE ID : CVE-2019-3475		
mopcms					
mopcms					
N/A	22-02-2019	6.4	A Path Traversal vulnerability was discovered in MOPCMS through 2018-11-30, leading to deletion of unexpected critical files. The exploitation point is in the "column management" function. The path added to the column is not verified. When a column is deleted by an attacker, the corresponding directory is deleted, as demonstrated by ./ to delete the entire web site. CVE ID : CVE-2019-9015	N/A	A-MOP-MOPC-030419/171
N/A	22-02-2019	4.3	An XSS vulnerability was discovered in MOPCMS through 2018-11-30. There is persistent XSS that allows remote attackers to inject arbitrary web script or HTML via the form[name] parameter in a mod=column request, as demonstrated by the /mopcms/X0AZgf(index).php?mod=column&ac=list&menuid=28&ac=add&menuid=29 URI. CVE ID : CVE-2019-9016	N/A	A-MOP-MOPC-030419/172
Netapp					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Snapdrive									
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559	https://www.openssl.org/news/secadv/20190226.txt	A-NET-SNAP-030419/173				
element_software									
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and	https://www.openssl.org/news/secadv/20190226.txt	A-NET-ELEM-030419/174				
CV Scoring Scale (CVSS)									
0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559	v/20190226.txt	
N/A	23-02-2019	6.8	An issue was discovered in GNU Binutils 2.32. It is a heap-based buffer overflow in process_mips_specific in readelf.c via a malformed MIPS option section. CVE ID : CVE-2019-9077	N/A	A-NET-ELEM-030419/175
hyper_converged_infrastructure					
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then	https://www.opens	A-NET-HYPE-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			<p>calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).</p> <p>CVE ID : CVE-2019-1559</p>	sl.org/news/secadv/20190226.txt	030419/176						
oncommand_unified_manager											
N/A	27-02-2019	4.3	<p>If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is</p>	https://www.openssl.org/news/secadv/20190226.txt	A-NET-ONCO-030419/177						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559								
oncommand_workflow_automation											
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the	https://www.openssl.org/news/secadv/20190226.txt	A-NET-ONCO-030419/178						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559		

ontap_select_deploy

N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched	https://www.openssl.org/news/secadv/20190226.txt	A-NET-ONTA-030419/179
-----	------------	-----	---	---	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559								
ontap_select_deploy_administration_utility											
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred	https://www.openssl.org/news/secadv/20190226.txt	A-NET-ONTA-030419/180						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559		
N/A	25-02-2019	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match. CVE ID : CVE-2019-9169	N/A	A-NET-ONTA-030419/181
santricity_smi-s_provider					
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites.	https://www.openssl.org/news/secadv/20190226.txt	A-NET-SANT-030419/182

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559		

steelstore_cloud_integrated_storage

N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-	https://www.openssl.org/news/secadv/20190226.txt	A-NET-STEE-030419/183
-----	------------	-----	--	---	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1.0.2q). CVE ID : CVE-2019-1559		
N/A	25-02-2019	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match. CVE ID : CVE-2019-9169	N/A	A-NET-STEE-030419/184
storagegrid					
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred	https://www.openssl.org/news/secadv/20190226.txt	A-NET-STOR-030419/185

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			(applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559								
element_software_management											
N/A	23-02-2019	6.8	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a heap-based buffer over-read in d_expression_1 in cp-demangle.c after many recursive calls. CVE ID : CVE-2019-9070	N/A	A-NET-ELEM-030419/186						
N/A	23-02-2019	4.3	An issue was discovered in GNU libiberty, as distributed in GNU Binutils 2.32. It is a stack consumption issue in d_count_templates_scopes in cp-demangle.c after many recursive calls. CVE ID : CVE-2019-9071	N/A	A-NET-ELEM-030419/187						
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in setup_group in elf.c. CVE ID : CVE-2019-9072	N/A	A-NET-ELEM-030419/188						
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in	N/A	A-NET-ELEM-030419/189						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			_bfd_elf_slurp_version_tables in elf.c. CVE ID : CVE-2019-9073							
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an out-of-bounds read leading to a SEGV in bfd_getl32 in libbfd.c, when called from pex64_get_runtime_function in pei-x86_64.c. CVE ID : CVE-2019-9074	N/A	A-NET-ELEM-030419/190					
N/A	23-02-2019	6.8	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is a heap-based buffer overflow in _bfd_archive_64_bit_slurp_armap in archive64.c. CVE ID : CVE-2019-9075	N/A	A-NET-ELEM-030419/191					
N/A	23-02-2019	4.3	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.32. It is an attempted excessive memory allocation in elf_read_notes in elf.c. CVE ID : CVE-2019-9076	N/A	A-NET-ELEM-030419/192					
cloud_backup										
N/A	25-02-2019	7.5	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an	N/A	A-NET-CLOU-030419/193					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			attempted case-insensitive regular-expression match. CVE ID : CVE-2019-9169								
clustered_data_ontap											
N/A	27-02-2019	5	Clustered Data ONTAP versions prior to 9.1P15 and 9.3 prior to 9.3P7 are susceptible to a vulnerability which discloses sensitive information to an unauthenticated user. CVE ID : CVE-2019-5491	https://security.netapp.com/advisory/ontap-20190227-0001/	A-NET-CLUS-030419/194						
Nvidia											
gpu_driver											
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display driver contains a vulnerability in the 3D vision component in which the stereo service software, when opening a file, does not check for hard links. This behavior may lead to code execution, denial of service or escalation of privileges. CVE ID : CVE-2019-5665	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/195						
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) create context command DDI DxgkDdiCreateContext in which the product uses untrusted input when calculating or using an array index, but the product does not validate or incorrectly validates the index to ensure the index references a valid position within the array, which may	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/196						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to denial of service or escalation of privileges. CVE ID : CVE-2019-5666		
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiSetRootPageTable in which the application dereferences a pointer that it expects to be valid, but is NULL, which may lead to code execution, denial of service or escalation of privileges. CVE ID : CVE-2019-5667	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/197
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiSubmitCommandVirtual in which the application dereferences a pointer that it expects to be valid, but is NULL, which may lead to denial of service or escalation of privileges. CVE ID : CVE-2019-5668	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/198
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiEscape in which the software uses a sequential operation to read from or write to a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/199

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the buffer, which may lead to denial of service or escalation of privileges. CVE ID : CVE-2019-5669		
N/A	27-02-2019	7.2	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer handler for DxgkDdiEscape in which the software uses a sequential operation to read from or write to a buffer, but it uses an incorrect length value that causes it to access memory that is outside of the bounds of the buffer which may lead to denial of service, escalation of privileges, code execution or information disclosure. CVE ID : CVE-2019-5670	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/200
N/A	27-02-2019	4.9	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape in which the software does not release a resource after its effective lifetime has ended, which may lead to denial of service. CVE ID : CVE-2019-5671	https://nvidia.custhelp.com/app/answers/detail/a_id/4772	A-NVI-GPU_-030419/201
octopus					
octopus_deploy					
N/A	19-02-2019	4	An Information Exposure issue in the Terraform deployment step in Octopus Deploy before 2019.1.8 (and before 2018.10.4 LTS) allows remote	N/A	A-OCT-OCTO-030419/202

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated users to view sensitive Terraform output variables via log files. CVE ID : CVE-2019-8944		
O-dyn					
Collabtive					
N/A	19-02-2019	3.5	Collabtive 3.1 allows XSS via the manageuser.php?action=profile id parameter. CVE ID : CVE-2019-8935	N/A	A-O-D-COLL-030419/203
onefilecms_project					
onefilecms					
N/A	17-02-2019	4	OneFileCMS 3.6.13 allows remote attackers to modify onefilecms.php by clicking the Copy button twice. CVE ID : CVE-2019-8408	N/A	A-ONE-ONEF-030419/204
online_food_ordering_script_project					
online_food_ordering_script					
N/A	23-02-2019	6	PHP Scripts Mall Online Food Ordering Script 1.0 has Cross-Site Request Forgery (CSRF) in my-account.php. CVE ID : CVE-2019-9062	N/A	A-ONL-ONLI-030419/205
opensourcebms					
open_source_background_management_system					
N/A	24-02-2019	10	ThinkPHP before 3.2.4, as used in Open Source BMS v1.1.1 and other products, allows Remote Command Execution via public/?s=index/\think\app\i nvokefunction&function=call_us er_func_array&vars[0]=system&	N/A	A-OPE-OPEN-030419/206

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vars[1][]= followed by the command. CVE ID : CVE-2019-9082		
Openssl					
Openssl					
N/A	27-02-2019	4.3	<p>If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).</p> <p>CVE ID : CVE-2019-1559</p>	https://www.openssl.org/news/secadv/20190226.txt	A-OPE-OPEN-030419/207

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ory					
hydra					
N/A	17-02-2019	4.3	ORY Hydra before v1.0.0-rc.3+oryOS.9 has Reflected XSS via the oauth2/fallbacks/error_error_hint parameter. CVE ID : CVE-2019-8400	N/A	A-ORY-HYDR-030419/208
pangea-comm					
fax_ata					
N/A	28-02-2019	7.8	Pangea Communications Internet FAX ATA all Versions 3.1.8 and prior allow an attacker to bypass user authentication using a specially crafted URL to cause the device to reboot, which may be used to cause a continual denial-of-service condition. CVE ID : CVE-2019-6551	N/A	A-PAN-FAX_-030419/209
Papercut					
papercut_mf					
N/A	19-02-2019	7.5	PaperCut MF before 18.3.6 and PaperCut NG before 18.3.6 allow script injection via the user interface, aka PC-15163. CVE ID : CVE-2019-8948	N/A	A-PAP-PAPE-030419/210
papercut_ng					
N/A	19-02-2019	7.5	PaperCut MF before 18.3.6 and PaperCut NG before 18.3.6 allow script injection via the user interface, aka PC-15163. CVE ID : CVE-2019-8948	N/A	A-PAP-PAPE-030419/211
Pbootcms					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pbootcms					
N/A	17-02-2019	6.5	A SQL Injection vulnerability exists in PbootCMS v1.3.2 via the description parameter in apps\admin\controller\content\ContentController.php. CVE ID : CVE-2019-8422	N/A	A-PBO-PBOO-030419/212
PHP					
PHP					
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. CVE ID : CVE-2019-9020	N/A	A-PHP-PHP-030419/213
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in	N/A	A-PHP-PHP-030419/214

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ext/phar/phar.c. CVE ID : CVE-2019-9021		
N/A	22-02-2019	5	An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries. CVE ID : CVE-2019-9022	N/A	A-PHP-PHP-030419/215
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte	N/A	A-PHP-PHP-030419/216

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sequences. CVE ID : CVE-2019-9023		
N/A	22-02-2019	5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c. CVE ID : CVE-2019-9024	N/A	A-PHP-PHP-030419/217
php_appointment_booking_script_project					
php_appointment_booking_script					
N/A	23-02-2019	3.5	PHP Scripts Mall PHP Appointment Booking Script 3.0.3 allows HTML injection in a user profile. CVE ID : CVE-2019-9066	N/A	A-PHP-PHP_-030419/218
phpmywind					
phpmywind					
N/A	17-02-2019	3.5	admin/default.php in PHPMyWind v5.5 has XSS via an HTTP Host header. CVE ID : CVE-2019-8435	N/A	A-PHP-PHPM-030419/219
pixeline					
bugs					
N/A	22-02-2019	7.5	An issue was discovered in Tiny Issue 1.3.1 and pixeline Bugs through 1.3.2c. install/config-setup.php allows remote attackers to execute arbitrary PHP code via the database_host	N/A	A-PIX-BUGS-030419/220

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter if the installer remains present in its original directory after installation is completed. CVE ID : CVE-2019-9002		

Pluck-cms

Pluck

N/A	23-02-2019	5.8	An issue was discovered in Pluck 4.7.9-dev1. There is a CSRF vulnerability that can delete a theme (aka topic) via a /admin.php?action=theme_delete&var1= URI. CVE ID : CVE-2019-9048	N/A	A-PLU-PLUC-030419/221
N/A	23-02-2019	5.8	An issue was discovered in Pluck 4.7.9-dev1. There is a CSRF vulnerability that can delete modules via a /admin.php?action=module_delete&var1= URI. CVE ID : CVE-2019-9049	N/A	A-PLU-PLUC-030419/222
N/A	23-02-2019	6.5	An issue was discovered in Pluck 4.7.9-dev1. It allows administrators to execute arbitrary code by using action=installmodule to upload a ZIP archive, which is then extracted and executed. CVE ID : CVE-2019-9050	N/A	A-PLU-PLUC-030419/223
N/A	23-02-2019	5.8	An issue was discovered in Pluck 4.7.9-dev1. There is a CSRF vulnerability that can delete articles via a /admin.php?action=deletepage&var1= URI.	N/A	A-PLU-PLUC-030419/224

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9051		
N/A	23-02-2019	5.8	An issue was discovered in Pluck 4.7.9-dev1. There is a CSRF vulnerability that can delete pictures via a /admin.php?action=deleteimage&var1= URI. CVE ID : CVE-2019-9052	N/A	A-PLU-PLUC-030419/225
podofo_project					
podofo					
N/A	26-02-2019	6.8	PoDoFo::Impose::PdfTranslator::setSource() in pdftranslator.cpp in PoDoFo 0.9.6 has a NULL pointer dereference that can (for example) be triggered by sending a crafted PDF file to the podofoimpose binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9199	N/A	A-POD-PODO-030419/226
Qemu					
Qemu					
N/A	19-02-2019	2.1	QEMU, through version 2.10 and through version 3.1.0, is vulnerable to an out-of-bounds read of up to 128 bytes in the hw/i2c/i2c-ddc.c:i2c_ddc() function. A local attacker with permission to execute i2c commands could exploit this to read stack memory of the qemu process on the host.	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3812	A-QEM-QEMU-030419/227

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-3812							
responsive_video_news_script_project										
responsive_video_news_script										
N/A	16-02-2019	4.3	PHP Scripts Mall Responsive Video News Script has XSS via the Search Bar. This might, for example, be leveraged for HTML injection or URL redirection. CVE ID : CVE-2019-8361	N/A	A-RES-RESP-030419/228					
schoolcms										
schoolcms										
N/A	26-02-2019	6.5	SchoolCMS version 2.3.1 allows file upload via the logo upload feature at admin.php?m=admin&c=site&a=save by using the .jpg extension, changing the Content-Type to image/php, and placing PHP code after the JPEG data. This ultimately allows execution of arbitrary PHP code. CVE ID : CVE-2019-9181	N/A	A-SCH-SCHO-030419/229					
S-cms										
S-cms										
N/A	23-02-2019	6.8	S-CMS PHP v3.0 has a CSRF vulnerability to add a new admin user via the admin/ajax.php?type=admin&action=add URI, a related issue to CVE-2018-19332. CVE ID : CVE-2019-9040	N/A	A-S-C-S-CM-030419/230					
seacms										
seacms										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
N/A	17-02-2019	4	SeaCMS 7.2 mishandles member.php?mod=repsw4 requests. CVE ID : CVE-2019-8418	N/A	A-SEA-SEAC-030419/231					
seafile										
seadroid										
N/A	18-02-2019	5	The seadroid (aka Seafile Android Client) application through 2.2.13 for Android always uses the same Initialization Vector (IV) with Cipher Block Chaining (CBC) Mode to encrypt private data, making it easier to conduct chosen-plaintext attacks or dictionary attacks. CVE ID : CVE-2019-8919	N/A	A-SEA-SEAD-030419/232					
sitemagic										
sitemagic_cms										
N/A	23-02-2019	6.5	An issue was discovered in Sitemagic CMS v4.4. In the index.php?SMExt=SMFiles URI, the user can upload a .php file to execute arbitrary code, as demonstrated by 404.php. CVE ID : CVE-2019-9042	N/A	A-SIT-SITE-030419/233					
Solarwinds										
orion_network_performance_monitor										
N/A	18-02-2019	10	SolarWinds Orion NPM before 12.4 suffers from a SYSTEM remote code execution vulnerability in the OrionModuleEngine service. This service establishes a NetTcpBinding endpoint that	N/A	A-SOL-ORIO-030419/234					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			allows remote, unauthenticated clients to connect and call publicly exposed methods. The InvokeActionMethod method may be abused by an attacker to execute commands as the SYSTEM user. CVE ID : CVE-2019-8917							
Splunk										
Splunk										
N/A	20-02-2019	3.5	Splunk Web in Splunk Enterprise 6.5.x before 6.5.5, 6.4.x before 6.4.9, 6.3.x before 6.3.12, 6.2.x before 6.2.14, 6.1.x before 6.1.14, and 6.0.x before 6.0.15 and Splunk Light before 6.6.0 has Persistent XSS, aka SPL-138827. CVE ID : CVE-2019-5727	N/A	A-SPL-SPLU-030419/235					
Sqlalchemy										
Sqlalchemy										
N/A	19-02-2019	7.5	SQLAlchemy through 1.2.17 and 1.3.x through 1.3.0b2 allows SQL Injection via the order_by parameter. CVE ID : CVE-2019-7164	N/A	A-SQL-SQLA-030419/236					
std42										
elfinder										
N/A	26-02-2019	7.5	elFinder before 2.1.48 has a command injection vulnerability in the PHP connector. CVE ID : CVE-2019-9194	N/A	A-STD-ELFI-030419/237					
sublimetext										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sublime_text_3					
N/A	25-02-2019	6.8	<p>** DISPUTED ** DLL hijacking is possible in Sublime Text 3 version 3.1.1 build 3176 on 32-bit Windows platforms because a Trojan horse api-ms-win-core-fibers-l1-1-1.dll or api-ms-win-core-localization-l1-2-1.dll file may be loaded if a victim uses sublime_text.exe to open a .txt file within an attacker's %LOCALAPPDATA%\Temp\sublime_text folder. NOTE: the vendor's position is "This does not appear to be a bug with Sublime Text, but rather one with Windows that has been patched."</p> <p>CVE ID : CVE-2019-9116</p>	N/A	A-SUB-SUBL-030419/238
tautulli					
tautulli					
N/A	19-02-2019	4.3	<p>data/interfaces/default/history.html in Tautulli 2.1.26 has XSS via a crafted Plex username that is mishandled when constructing the History page.</p> <p>CVE ID : CVE-2019-8939</p>	N/A	A-TAU-TAUT-030419/239
themerig					
find_a_place cms_directory					
N/A	16-02-2019	7.5	<p>Themerig Find a Place CMS Directory 1.5 has SQL Injection via the find/assets/external/data_2.php cate parameter.</p> <p>CVE ID : CVE-2019-8360</p>	N/A	A-THE-FIND-030419/240

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tintin_project					
tintin					
N/A	18-02-2019	7.5	Stack-based buffer overflow in the strip_vt102_codes function in TinTin++ 2.01.6 and WinTin++ 2.01.6 allows remote attackers to execute arbitrary code by sending a long message to the client. CVE ID : CVE-2019-7629	N/A	A-TIN-TINT-030419/241
wintin					
N/A	18-02-2019	7.5	Stack-based buffer overflow in the strip_vt102_codes function in TinTin++ 2.01.6 and WinTin++ 2.01.6 allows remote attackers to execute arbitrary code by sending a long message to the client. CVE ID : CVE-2019-7629	N/A	A-TIN-WINT-030419/242
tiny_issue_project					
tiny_issue					
N/A	22-02-2019	7.5	An issue was discovered in Tiny Issue 1.3.1 and pixeline Bugs through 1.3.2c. install/config-setup.php allows remote attackers to execute arbitrary PHP code via the database_host parameter if the installer remains present in its original directory after installation is completed. CVE ID : CVE-2019-9002	N/A	A-TIN-TINY-030419/243
Torproject					
TOR					

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	21-02-2019	5	In Tor before 0.3.3.12, 0.3.4.x before 0.3.4.11, 0.3.5.x before 0.3.5.8, and 0.4.x before 0.4.0.2-alpha, remote denial of service against Tor clients and relays can occur via memory exhaustion in the KIST cell scheduler. CVE ID : CVE-2019-8955	N/A	A-TOR-TOR-030419/244
txjia					
imcat					
N/A	17-02-2019	3.5	imcat 4.5 has Stored XSS via the root/run/adm.php fm[instop][note] parameter. CVE ID : CVE-2019-8436	N/A	A-TXJ-IMCA-030419/245
verydows					
verydows					
N/A	16-02-2019	4.3	Verydows 2.0 has XSS via the index.php?c=main a parameter, as demonstrated by an a=index[XSS] value. CVE ID : CVE-2019-8363	N/A	A-VER-VERY-030419/246
vnote_project					
vnote					
N/A	17-02-2019	4.3	VNote 2.2 has XSS via a new text note. CVE ID : CVE-2019-8419	N/A	A-VNO-VNOT-030419/247
wavemaker					
wavemaker_studio					
N/A	21-02-2019	6.8	com/wavemaker/studio/StudioService.java in WaveMaker Studio 6.6 mishandles the studioService.download?metho	N/A	A-WAV-WAVE-030419/248

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			d=getContent&inUrl= value, leading to disclosure of local files and SSRF. CVE ID : CVE-2019-8982		
Webkitgtk					
Webkitgtk					
N/A	24-02-2019	7.5	The UIProcess subsystem in WebKit, as used in WebKitGTK through 2.23.90 and WebKitGTK+ through 2.22.6 and other products, does not prevent the script dialog size from exceeding the web view size, which allows remote attackers to cause a denial of service (Buffer Overflow) or possibly have unspecified other impact, related to UIProcess/API/gtk/WebKitScriptDialogGtk.cpp, UIProcess/API/gtk/WebKitScriptDialogImpl.cpp, and UIProcess/API/gtk/WebKitWebViewGtk.cpp, as demonstrated by GNOME Web (aka Epiphany). CVE ID : CVE-2019-8375	N/A	A-WEB-WEBK-030419/249
Webkitgtk+					
N/A	24-02-2019	7.5	The UIProcess subsystem in WebKit, as used in WebKitGTK through 2.23.90 and WebKitGTK+ through 2.22.6 and other products, does not prevent the script dialog size from exceeding the web view size, which allows remote attackers to cause a denial of	N/A	A-WEB-WEBK-030419/250

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (Buffer Overflow) or possibly have unspecified other impact, related to UIProcess/API/gtk/WebKitScriptDialogGtk.cpp, UIProcess/API/gtk/WebKitScriptDialogImpl.cpp, and UIProcess/API/gtk/WebKitWebViewGtk.cpp, as demonstrated by GNOME Web (aka Epiphany). CVE ID : CVE-2019-8375		

Wireshark

Wireshark

N/A	27-02-2019	5	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the TCAP dissector could crash. This was addressed in epan/dissectors/asn1/tcap/tcap.cnf by avoiding NULL pointer dereferences. CVE ID : CVE-2019-9208	N/A	A-WIR-WIRE-030419/251
N/A	27-02-2019	5	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the ASN.1 BER and related dissectors could crash. This was addressed in epan/dissectors/packet-ber.c by preventing a buffer overflow associated with excessive digits in time values. CVE ID : CVE-2019-9209	N/A	A-WIR-WIRE-030419/252
N/A	27-02-2019	5	In Wireshark 2.4.0 to 2.4.12 and 2.6.0 to 2.6.6, the RPCAP dissector could crash. This was addressed in epan/dissectors/packet-rpcap.c by avoiding an attempted	N/A	A-WIR-WIRE-030419/253

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dereference of a NULL conversation. CVE ID : CVE-2019-9214		
Woocommerce					
Woocommerce					
N/A	25-02-2019	4.3	WooCommerce before 3.5.5 allows XSS via a Photoswipe caption. CVE ID : CVE-2019-9168	N/A	A-WOO-WOOC-030419/254
Wordpress					
Wordpress					
N/A	19-02-2019	6.5	WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943. CVE ID : CVE-2019-8942	N/A	A-WOR-WORD-030419/255
N/A	19-02-2019	4	WordPress through 5.0.3 allows Path Traversal in wp_crop_image(). An attacker (who has privileges to crop an image) can write the output image to an arbitrary directory via a filename containing two image extensions and ../ sequences, such as a filename	N/A	A-WOR-WORD-030419/256

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ending with the .jpg?/././file.jpg substring. CVE ID : CVE-2019-8943		
wtcms_project					
wtcms					
N/A	18-02-2019	7.5	An issue was discovered in WTCMS 1.0. It allows remote attackers to execute arbitrary PHP code by going to the "Setting -> Mailbox configuration -> Registration email template" screen, and uploading an image file, as demonstrated by a .php filename and the "Content-Type: image/gif" header. CVE ID : CVE-2019-8908	N/A	A-WTC-WTCM-030419/257
N/A	18-02-2019	5	An issue was discovered in WTCMS 1.0. It allows remote attackers to cause a denial of service (resource consumption) via crafted dimensions for the verification code image. CVE ID : CVE-2019-8909	N/A	A-WTC-WTCM-030419/258
N/A	18-02-2019	6.8	An issue was discovered in WTCMS 1.0. It allows index.php?g=admin&m=setting &a=site_post CSRF. CVE ID : CVE-2019-8910	N/A	A-WTC-WTCM-030419/259
N/A	18-02-2019	4.3	An issue was discovered in WTCMS 1.0. It has stored XSS via the third text box (for the website statistics code). CVE ID : CVE-2019-8911	N/A	A-WTC-WTCM-030419/260

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
wuzhicms										
wuzhi_cms										
N/A	24-02-2019	4.3	XSS exists in WUZHI CMS 4.1.0 via index.php?m=attachment&f=im agecut&v=init&imgurl=[XSS] to coreframe/app/attachment/im agecut.php. CVE ID : CVE-2019-9107	N/A	A-WUZ- WUZH- 030419/261					
N/A	24-02-2019	4.3	XSS exists in WUZHI CMS 4.1.0 via index.php?m=message&f=mess age&v=add&username=[XSS] to coreframe/app/message/messa ge.php. CVE ID : CVE-2019-9109	N/A	A-WUZ- WUZH- 030419/262					
N/A	24-02-2019	4.3	XSS exists in WUZHI CMS 4.1.0 via index.php?m=content&f=postinf o&v=listing&set_iframe=[XSS] to coreframe/app/content/postinf o.php. CVE ID : CVE-2019-9110	N/A	A-WUZ- WUZH- 030419/263					
wuzhicms										
N/A	24-02-2019	4.3	XSS exists in WUZHI CMS 4.1.0 via index.php?m=core&f=map&v=b aidumap&x=[XSS]&y=[XSS] to coreframe/app/core/map.php. CVE ID : CVE-2019-9108	N/A	A-WUZ- WUZH- 030419/264					
Zoneminder										
Zoneminder										
N/A	17-02-2019	7.5	ZoneMinder through 1.32.3 has	N/A	A-ZON-					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SQL Injection via the skins/classic/views/events.php filter[Query][terms][0][cnj] parameter. CVE ID : CVE-2019-8423		ZONE-030419/265
N/A	17-02-2019	7.5	ZoneMinder before 1.32.3 has SQL Injection via the ajax/status.php sort parameter. CVE ID : CVE-2019-8424	N/A	A-ZON-ZONE-030419/266
N/A	17-02-2019	4.3	includes/database.php in ZoneMinder before 1.32.3 has XSS in the construction of SQL-ERR messages. CVE ID : CVE-2019-8425	N/A	A-ZON-ZONE-030419/267
N/A	17-02-2019	4.3	skins/classic/views/controlcap.php in ZoneMinder before 1.32.3 has XSS via the newControl array, as demonstrated by the newControl[MinTiltRange] parameter. CVE ID : CVE-2019-8426	N/A	A-ZON-ZONE-030419/268
N/A	17-02-2019	7.5	daemonControl in includes/functions.php in ZoneMinder before 1.32.3 allows command injection via shell metacharacters. CVE ID : CVE-2019-8427	N/A	A-ZON-ZONE-030419/269
N/A	17-02-2019	7.5	ZoneMinder before 1.32.3 has SQL Injection via the skins/classic/views/control.php groupSql parameter, as demonstrated by a newGroup[MonitorIds][] value. CVE ID : CVE-2019-8428	N/A	A-ZON-ZONE-030419/270

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	17-02-2019	7.5	ZoneMinder before 1.32.3 has SQL Injection via the ajax/status.php filter[Query][terms][0][cnj] parameter. CVE ID : CVE-2019-8429	N/A	A-ZON-ZONE-030419/271
zzcms					
zzcms					
N/A	17-02-2019	6.4	admin/dl_data.php in zzcms 2018 (2018-10-19) allows remote attackers to delete arbitrary files via action=del&filename=../ directory traversal. CVE ID : CVE-2019-8411	N/A	A-ZZC-ZZCM-030419/272
N/A	24-02-2019	3.5	zzcms 2019 has XSS via an arbitrary user/ask.php?do=modify parameter because inc/stopsqlin.php does not block a mixed-case string such as sCrIpT. CVE ID : CVE-2019-9078	N/A	A-ZZC-ZZCM-030419/273
zzzcms					
zzzphp					
N/A	23-02-2019	6.5	An issue was discovered in ZZZCMS zzzphp V1.6.1. In the inc/zzz_template.php file, the parserIfLabel() function's filtering is not strict, resulting in PHP code execution, as demonstrated by the if:assert substring. CVE ID : CVE-2019-9041	N/A	A-ZZZ-ZZZP-030419/274

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	24-02-2019	10	ThinkPHP before 3.2.4, as used in Open Source BMS v1.1.1 and other products, allows Remote Command Execution via public/?s=index/\think\app/invokefunction&function=call_user_func_array&vars[0]=system&vars[1][]= followed by the command. CVE ID : CVE-2019-9082	N/A	A-ZZZ-ZZZP-030419/275
N/A	26-02-2019	6.8	There is a CSRF in ZZZCMS zzzphp V1.6.1 via a /admin015/save.php?act=editfile request. It allows PHP code injection by providing a filename in the file parameter, and providing file content in the filetext parameter. CVE ID : CVE-2019-9182	N/A	A-ZZZ-ZZZP-030419/276
OS					
Canonical					
ubuntu_linux					
N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the	https://www.openssl.org/news/secadv/20190226.txt	O-CAN-UBUN-030419/277

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559		
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. CVE ID : CVE-2019-9020	N/A	O-CAN-UBUN-030419/278
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker	N/A	O-CAN-UBUN-030419/279

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c. CVE ID : CVE-2019-9021		
N/A	22-02-2019	5	An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries. CVE ID : CVE-2019-9022	N/A	O-CAN-UBUN-030419/280
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regpa	N/A	O-CAN-UBUN-030419/281

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			rse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences. CVE ID : CVE-2019-9023							
N/A	22-02-2019	5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c. CVE ID : CVE-2019-9024	N/A	O-CAN-UBUN-030419/282					
N/A	26-02-2019	6.8	A heap-based buffer underwrite exists in ImageStream::getLine() located at Stream.cc in Poppler 0.74.0 that can (for example) be triggered by sending a crafted PDF file to the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9200	N/A	O-CAN-UBUN-030419/283					
Cisco										
rv110w_firmware										
N/A	28-02-2019	10	A vulnerability in the web-based management interface of the	N/A	O-CIS-RV11-030419/284					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. RV110W Wireless-N VPN Firewall versions prior to 1.2.2.1 are affected. RV130W Wireless-N Multifunction VPN Router versions prior to 1.0.3.45 are affected. RV215W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663							
rv130w_firmware										
N/A	28-02-2019	10	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could	N/A	O-CIS-RV13-030419/285					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. RV110W Wireless-N VPN Firewall versions prior to 1.2.2.1 are affected. RV130W Wireless-N Multifunction VPN Router versions prior to 1.0.3.45 are affected. RV215W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663							
rv215w_firmware										
N/A	28-02-2019	10	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-	N/A	O-CIS-RV21-030419/286					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			supplied data in the web-based management interface. An attacker could exploit this vulnerability by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. RV110W Wireless-N VPN Firewall versions prior to 1.2.2.1 are affected. RV130W Wireless-N Multifunction VPN Router versions prior to 1.0.3.45 are affected. RV215W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663								
hyperflex_hx_data_platform											
N/A	21-02-2019	7.2	A vulnerability in the hxterm service of Cisco HyperFlex Software could allow an unauthenticated, local attacker to gain root access to all nodes in the cluster. The vulnerability is due to insufficient authentication controls. An attacker could exploit this vulnerability by connecting to the hxterm service as a non-privileged, local user. A successful exploit could allow the attacker to gain root access to all member nodes of the HyperFlex cluster. This vulnerability affects Cisco	N/A	O-CIS-HYPE-030419/287						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HyperFlex Software Releases prior to 3.5(2a). CVE ID : CVE-2019-1664		
N/A	21-02-2019	4.3	A vulnerability in the web-based management interface of Cisco HyperFlex software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected system. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Versions prior to 3.5(1a) are affected. CVE ID : CVE-2019-1665	N/A	O-CIS-HYPE-030419/288
N/A	21-02-2019	5	A vulnerability in the Graphite service of Cisco HyperFlex software could allow an unauthenticated, remote attacker to retrieve data from the Graphite service. The vulnerability is due to insufficient authentication	N/A	O-CIS-HYPE-030419/289

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controls. An attacker could exploit this vulnerability by sending crafted requests to the Graphite service. A successful exploit could allow the attacker to retrieve any statistics from the Graphite service. Versions prior to 3.5(2a) are affected. CVE ID : CVE-2019-1666		
N/A	21-02-2019	2.1	A vulnerability in the Graphite interface of Cisco HyperFlex software could allow an authenticated, local attacker to write arbitrary data to the Graphite interface. The vulnerability is due to insufficient authorization controls. An attacker could exploit this vulnerability by connecting to the Graphite service and sending arbitrary data. A successful exploit could allow the attacker to write arbitrary data to Graphite, which could result in invalid statistics being presented in the interface. Versions prior to 3.5(2a) are affected. CVE ID : CVE-2019-1667	N/A	O-CIS-HYPE-030419/290
ios_xr					
N/A	21-02-2019	5	A vulnerability in the TFTP service of Cisco Network Convergence System 1000 Series software could allow an unauthenticated, remote attacker to retrieve arbitrary files from the targeted device,	N/A	O-CIS-IOS_-030419/291

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			possibly resulting in information disclosure. The vulnerability is due to improper validation of user-supplied input within TFTP requests processed by the affected software. An attacker could exploit this vulnerability by using directory traversal techniques in malicious requests sent to the TFTP service on a targeted device. An exploit could allow the attacker to retrieve arbitrary files from the targeted device, resulting in the disclosure of sensitive information. This vulnerability affects Cisco IOS XR Software releases prior to Release 6.5.2 for Cisco Network Convergence System 1000 Series devices when the TFTP service is enabled. CVE ID : CVE-2019-1681							
spa112_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could	N/A	O-CIS-SPA1-030419/292					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones.</p> <p>CVE ID : CVE-2019-1683</p>		

spa500_firmware

N/A	25-02-2019	5.8	<p>A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially</p>	N/A	0-CIS-SPA5-030419/293
-----	------------	-----	---	-----	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683		

spa500ds_firmware

N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5	N/A	O-CIS-SPA5-030419/294
-----	------------	-----	---	-----	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683		
spa500s_firmware					
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones.	N/A	O-CIS-SPA5-030419/295

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			CVE ID : CVE-2019-1683							
spa501g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683	N/A	O-CIS-SPA5-030419/296					
spa502g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and	N/A	O-CIS-SPA5-030419/297					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683							
spa504g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation	N/A	O-CIS-SPA5-030419/298					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones.</p> <p>CVE ID : CVE-2019-1683</p>		

spa508g_firmware

N/A	25-02-2019	5.8	<p>A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server</p>	N/A	O-CIS-SPA5-030419/299
-----	------------	-----	--	-----	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683							
spa509g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected	N/A	O-CIS-SPA5-030419/300					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683								
spa512g_firmware											
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business	N/A	O-CIS-SPA5-030419/301						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683							
spa514g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683	N/A	O-CIS-SPA5-030419/302					
spa525_firmware										
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683	N/A	O-CIS-SPA5-030419/303					
spa525g_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or	N/A	O-CIS-SPA5-030419/304					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sqli- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683							
spa5x5_firmware										
N/A	25-02-2019	5.8	A vulnerability in the certificate handling component of the Cisco SPA112, SPA525, and SPA5X5 Series IP Phones could allow an unauthenticated, remote attacker to listen to or control some aspects of a Transport Level Security (TLS)-encrypted Session Initiation Protocol (SIP) conversation. The vulnerability is due to the improper validation of server	N/A	O-CIS-SPA5-030419/305					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certificates. An attacker could exploit this vulnerability by crafting a malicious server certificate to present to the client. An exploit could allow an attacker to eavesdrop on TLS-encrypted traffic and potentially route or redirect calls initiated by an affected device. Affected software include version 7.6.2 of the Cisco Small Business SPA525 Series IP Phones and Cisco Small Business SPA5X5 Series IP Phones and version 1.4.2 of the Cisco Small Business SPA500 Series IP Phones and Cisco Small Business SPA112 Series IP Phones. CVE ID : CVE-2019-1683		

firepower_9000_firmware

N/A	21-02-2019	5.7	A vulnerability in field-programmable gate array (FPGA) ingress buffer management for the Cisco Firepower 9000 Series with the Cisco Firepower 2-port 100G double-width network module (PID: FPR9K-DNM-2X100G) could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. Manual intervention may be required before a device will resume normal operations. The vulnerability is due to a logic error in the FPGA related to the processing of different types of input packets. An	N/A	O-CIS-FIRE-030419/306
-----	------------	-----	---	-----	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<p>attacker could exploit this vulnerability by being on the adjacent subnet and sending a crafted sequence of input packets to a specific interface on an affected device. A successful exploit could allow the attacker to cause a queue wedge condition on the interface. When a wedge occurs, the affected device will stop processing any additional packets that are received on the wedged interface. Version 2.2 is affected.</p> <p>CVE ID : CVE-2019-1700</p>		

Citrix

netScaler_application_delivery_controller_firmware

N/A	22-02-2019	4.3	<p>Citrix NetScaler Gateway 12.1 before build 50.31, 12.0 before build 60.9, 11.1 before build 60.14, 11.0 before build 72.17, and 10.5 before build 69.5 and Application Delivery Controller (ADC) 12.1 before build 50.31, 12.0 before build 60.9, 11.1 before build 60.14, 11.0 before build 72.17, and 10.5 before build 69.5 allow remote attackers to obtain sensitive plaintext information because of a TLS Padding Oracle Vulnerability when CBC-based cipher suites are enabled.</p> <p>CVE ID : CVE-2019-6485</p>	N/A	O-CIT-NETS-030419/307
-----	------------	-----	---	-----	-----------------------

netScaler_gateway_firmware

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-02-2019	4.3	Citrix NetScaler Gateway 12.1 before build 50.31, 12.0 before build 60.9, 11.1 before build 60.14, 11.0 before build 72.17, and 10.5 before build 69.5 and Application Delivery Controller (ADC) 12.1 before build 50.31, 12.0 before build 60.9, 11.1 before build 60.14, 11.0 before build 72.17, and 10.5 before build 69.5 allow remote attackers to obtain sensitive plaintext information because of a TLS Padding Oracle Vulnerability when CBC-based cipher suites are enabled. CVE ID : CVE-2019-6485	N/A	O-CIT-NETS-030419/308

dasannetworks

h665_firmware

N/A	19-02-2019	10	The backdoor account dnsekakf2\$\$ in /bin/login on DASAN H665 devices with firmware 1.46p1-0028 allows an attacker to login to the admin account via TELNET. CVE ID : CVE-2019-8950	N/A	O-DAS-H665-030419/309
-----	------------	----	--	-----	-----------------------

Debian

debian_linux

N/A	27-02-2019	4.3	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is	https://www.openssl.org/news/secadv/20190226.txt	O-DEB-DEBI-030419/310
-----	------------	-----	--	---	-----------------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q). CVE ID : CVE-2019-1559		
N/A	19-02-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy. CVE ID : CVE-2019-5754	N/A	O-DEB-DEBI-030419/311
N/A	19-02-2019	5.8	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a	N/A	O-DEB-DEBI-030419/312

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. CVE ID : CVE-2019-5755		
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5756	N/A	O-DEB-DEBI-030419/313
N/A	19-02-2019	6.8	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. CVE ID : CVE-2019-5757	N/A	O-DEB-DEBI-030419/314
N/A	19-02-2019	6.8	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5758	N/A	O-DEB-DEBI-030419/315
N/A	19-02-2019	6.8	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5759	N/A	O-DEB-DEBI-030419/316
N/A	19-02-2019	6.8	Insufficient checks of pointer	N/A	O-DEB-DEBI-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5760		030419/317
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5762	N/A	O-DEB-DEBI-030419/318
N/A	19-02-2019	6.8	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5763	N/A	O-DEB-DEBI-030419/319
N/A	19-02-2019	6.8	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5764	N/A	O-DEB-DEBI-030419/320
N/A	19-02-2019	4.3	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from	N/A	O-DEB-DEBI-030419/321

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process memory via a crafted Intent. CVE ID : CVE-2019-5765		
N/A	19-02-2019	4.3	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2019-5766	N/A	O-DEB-DEBI-030419/322
N/A	19-02-2019	4.3	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK. CVE ID : CVE-2019-5767	N/A	O-DEB-DEBI-030419/323
N/A	19-02-2019	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension. CVE ID : CVE-2019-5768	N/A	O-DEB-DEBI-030419/324
N/A	19-02-2019	6.8	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted	N/A	O-DEB-DEBI-030419/325

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTML page. CVE ID : CVE-2019-5769		
N/A	19-02-2019	6.8	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. CVE ID : CVE-2019-5770	N/A	O-DEB-DEBI-030419/326
N/A	19-02-2019	6.8	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2019-5772	N/A	O-DEB-DEBI-030419/327
N/A	19-02-2019	4.3	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. CVE ID : CVE-2019-5773	N/A	O-DEB-DEBI-030419/328
N/A	19-02-2019	6.8	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file. CVE ID : CVE-2019-5774	N/A	O-DEB-DEBI-030419/329

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5775	N/A	O-DEB-DEBI-030419/330
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5776	N/A	O-DEB-DEBI-030419/331
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5777	N/A	O-DEB-DEBI-030419/332
N/A	19-02-2019	4.3	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. CVE ID : CVE-2019-5778	N/A	O-DEB-DEBI-030419/333
N/A	19-02-2019	4.3	Insufficient policy validation in	N/A	O-DEB-DEBI-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2019-5779		030419/334
N/A	19-02-2019	4.6	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events. CVE ID : CVE-2019-5780	N/A	O-DEB-DEBI-030419/335
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5781	N/A	O-DEB-DEBI-030419/336
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2019-5782	N/A	O-DEB-DEBI-030419/337
N/A	19-02-2019	6.8	Missing URI encoding of untrusted input in DevTools in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform a Dangling Markup Injection attack via a crafted HTML page.	N/A	O-DEB-DEBI-030419/338

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5783		
N/A	18-02-2019	6.8	do_core_note in readelf.c in libmagic.a in file 5.35 has a stack-based buffer over-read, related to file_printable, a different vulnerability than CVE-2018-10360. CVE ID : CVE-2019-8905	N/A	O-DEB-DEBI-030419/339
N/A	18-02-2019	6.8	do_core_note in readelf.c in libmagic.a in file 5.35 allows remote attackers to cause a denial of service (stack corruption and application crash) or possibly have unspecified other impact. CVE ID : CVE-2019-8907	N/A	O-DEB-DEBI-030419/340
N/A	19-02-2019	6.5	WordPress before 4.9.9 and 5.x before 5.0.1 allows remote code execution because an _wp_attached_file Post Meta entry can be changed to an arbitrary string, such as one ending with a .jpg?file.php substring. An attacker with author privileges can execute arbitrary code by uploading a crafted image containing PHP code in the Exif metadata. Exploitation can leverage CVE-2019-8943. CVE ID : CVE-2019-8942	N/A	O-DEB-DEBI-030419/341
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can	N/A	O-DEB-DEBI-030419/342

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c. CVE ID : CVE-2019-9020		
N/A	22-02-2019	7.5	An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c. CVE ID : CVE-2019-9021	N/A	O-DEB-DEBI-030419/343
N/A	22-02-2019	5	An issue was discovered in PHP 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.2. dns_get_record misparses a DNS response, which can allow a hostile DNS server to cause PHP to misuse memcpy, leading to read operations going past the buffer allocated for DNS data. This affects php_parserr in ext/standard/dns.c for DNS_CAA and DNS_ANY queries. CVE ID : CVE-2019-9022	N/A	O-DEB-DEBI-030419/344

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-02-2019	7.5	<p>An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in</p> <p>ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.</p> <p>CVE ID : CVE-2019-9023</p>	N/A	O-DEB-DEBI-030419/345
N/A	22-02-2019	5	<p>An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in</p> <p>ext/xmlrpc/libxmlrpc/base64.c.</p> <p>CVE ID : CVE-2019-9024</p>	N/A	O-DEB-DEBI-030419/346
N/A	26-02-2019	6.8	<p>A heap-based buffer underwrite exists in</p>	N/A	O-DEB-DEBI-030419/347

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ImageStream::getLine() located at Stream.cc in Poppler 0.74.0 that can (for example) be triggered by sending a crafted PDF file to the pdftimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. CVE ID : CVE-2019-9200		
N/A	27-02-2019	4.3	In AdvanceCOMP 2.1, png_compress in pngex.cc in advpng has an integer overflow upon encountering an invalid PNG size, which results in an attempted memcpy to write into a buffer that is too small. (There is also a heap-based buffer over-read.) CVE ID : CVE-2019-9210	N/A	O-DEB-DEBI-030419/348

Dlink

dir-823g_firmware

N/A	16-02-2019	5	An issue was discovered on D-Link DIR-823G devices with firmware 1.02B03. There is incorrect access control allowing remote attackers to enable Guest Wi-Fi via the SetWlanRadioSettings HNAP API to the web service provided by /bin/goahead. CVE ID : CVE-2019-8392	N/A	O-DLI-DIR--030419/349
-----	------------	---	---	-----	-----------------------

D-link

dir-825_rev.b_firmware

N/A	25-02-2019	6.5	An issue was discovered on D-	N/A	O-D-L-DIR--
-----	------------	-----	-------------------------------	-----	-------------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Link DIR-825 Rev.B 2.10 devices. They allow remote attackers to execute arbitrary commands via the ntp_server parameter in an ntp_sync.cgi POST request. CVE ID : CVE-2019-9122		030419/350					
N/A	25-02-2019	7.5	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. The "user" account has a blank password. CVE ID : CVE-2019-9123	N/A	O-D-L-DIR--030419/351					
N/A	25-02-2019	5	An issue was discovered on D-Link DIR-825 Rev.B 2.10 devices. There is an information disclosure vulnerability via requests for the router_info.xml document. This will reveal the PIN code, MAC address, routing table, firmware version, update time, QOS information, LAN information, and WLAN information of the device. CVE ID : CVE-2019-9126	N/A	O-D-L-DIR--030419/352					
dir-878_firmware										
N/A	25-02-2019	7.5	An issue was discovered on D-Link DIR-878 1.12B01 devices. At the /HNAP1 URI, an attacker can log in with a blank password. CVE ID : CVE-2019-9124	N/A	O-D-L-DIR--030419/353					
N/A	25-02-2019	7.5	An issue was discovered on D-Link DIR-878 1.12B01 devices. Because strncpy is misused, there is a stack-based buffer overflow vulnerability that does	N/A	O-D-L-DIR--030419/354					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			not require authentication via the HNAP_AUTH HTTP header. CVE ID : CVE-2019-9125								
Google											
Android											
N/A	28-02-2019	9.3	In SkSwizzler::onSetSampleX of SkSwizzler.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege in system_server with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-117838472. CVE ID : CVE-2019-1986	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/355						
N/A	28-02-2019	9.3	In onSetSampleX of SkSwizzler.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-118143775. CVE ID : CVE-2019-1987	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/356						
N/A	28-02-2019	9.3	In sample6 of SkSwizzler.cpp, there is a possible out of bounds write due to improper input	https://source.android.com/	O-GOO-ANDR-030419/357						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation. This could lead to remote code execution in system_server with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-118372692. CVE ID : CVE-2019-1988	security/bulletin/2019-02-01	
N/A	28-02-2019	9.3	In btif_dm_data_copy of btif_core.cc, there is a possible out of bounds write due to a buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-110166268. CVE ID : CVE-2019-1991	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/358
N/A	28-02-2019	7.6	In bta_hl_sdp_query_results of bta_hl_main.cc, there is a possible use-after-free due to a race condition. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/359

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: A-116222069. CVE ID : CVE-2019-1992		
N/A	28-02-2019	7.2	In register_app of btif_hd.cc, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-119819889. CVE ID : CVE-2019-1993	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/360
N/A	28-02-2019	9.3	In refresh of DevelopmentTiles.java, there is the possibility of leaving development settings accessible due to an insecure default value. This could lead to unwanted access to development settings, with no additional execution privileges needed. User interaction is needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-117770924. CVE ID : CVE-2019-1994	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/361
N/A	28-02-2019	2.1	In ComposeActivityEmail of ComposeActivityEmail.java, there is a possible way to silently attach files to an email due to a confused deputy. This could lead to local information disclosure, sending files	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/362

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			accessible to AOSP Mail to a remote email recipient, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-32589229. CVE ID : CVE-2019-1995	01	
N/A	28-02-2019	3.3	In avrc_pars_browse_rsp of avrc_pars_ct.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-8.0 Android-8.1 Android-9. Android ID: A-111451066. CVE ID : CVE-2019-1996	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/363
N/A	28-02-2019	5	In random_get_bytes of random.c, there is a possible degradation of randomness due to an insecure default value. This could lead to local information disclosure via an insecure wireless connection with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-7.0 Android-	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/364

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.1.1 Android-7.1.2 Android-8.0 Android-8.1 Android-9. Android ID: A-117508900. CVE ID : CVE-2019-1997		
N/A	28-02-2019	4.9	In event_handler of keymaster_app.c, there is possible resource exhaustion due to a table being lost on reboot. This could lead to local denial of service that is not fixed by a factory reset, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android-9. Android ID: A-116055338. CVE ID : CVE-2019-1998	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/365
N/A	28-02-2019	7.2	In binder_alloc_free_page of binder_alloc.c, there is a possible double free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-120025196. CVE ID : CVE-2019-1999	N/A	O-GOO-ANDR-030419/366
N/A	28-02-2019	7.2	In several functions of binder.c, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges	N/A	O-GOO-ANDR-030419/367

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-120025789. CVE ID : CVE-2019-2000		
N/A	28-02-2019	2.1	The permissions on /proc/iomem were world-readable. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-117422211. CVE ID : CVE-2019-2001	https://source.android.com/security/bulletin/2019-02-01	O-GOO-ANDR-030419/368

Linux

linux_kernel

N/A	18-02-2019	7.2	In the Linux kernel through 4.20.11, af_alg_release() in crypto/af_alg.c neglects to set a NULL value for a certain structure member, which leads to a use-after-free in sockfs_setattr. CVE ID : CVE-2019-8912	N/A	O-LIN-LINU-030419/369
N/A	21-02-2019	7.8	A memory leak in the kernel_read_file function in fs/exec.c in the Linux kernel through 4.20.11 allows attackers to cause a denial of service (memory consumption) by triggering vfs_read failures. CVE ID : CVE-2019-8980	N/A	O-LIN-LINU-030419/370

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	22-02-2019	7.8	In the Linux kernel before 4.20.5, attackers can trigger a drivers/char/ipmi/ipmi_msg_handler.c use-after-free and OOPS by arranging for certain simultaneous execution of the code, as demonstrated by a "service ipmievmd restart" loop. CVE ID : CVE-2019-9003	N/A	O-LIN-LINU-030419/371
N/A	25-02-2019	4.6	In the Linux kernel before 4.20.12, net/ipv4/netfilter/nf_nat_snmp_basic_main.c in the SNMP NAT module has insufficient ASN.1 length checks (aka an array index error), making out-of-bounds read and write operations possible, leading to an OOPS or local privilege escalation. This affects snmp_version and snmp_helper. CVE ID : CVE-2019-9162	N/A	O-LIN-LINU-030419/372
micode					
xiaomi_perseus-p-oss					
N/A	24-02-2019	7.1	The msm gpu driver for custom Linux kernels on the Xiaomi perseus-p-oss MIX 3 device through 2018-11-26 has an integer overflow and OOPS because of missing checks of the count argument in sde_evtlog_filter_write in drivers/gpu/drm/msm/sde_dbg.c. This is exploitable for a device crash via a syscall by a crafted application on a rooted	N/A	O-MIC-XIAO-030419/373

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. CVE ID : CVE-2019-9111		
N/A	24-02-2019	7.1	The msm gpu driver for custom Linux kernels on the Xiaomi perseus-p-oss MIX 3 device through 2018-11-26 has an integer overflow and OOPS because of missing checks of the count argument in _sde_debugfs_conn_cmd_tx_write in drivers/gpu/drm/msm/sde/sde_connector.c. This is exploitable for a device crash via a syscall by a crafted application on a rooted device. CVE ID : CVE-2019-9112	N/A	O-MIC-XIAO-030419/374

Mikrotik

Routeros

N/A	20-02-2019	5	MikroTik RouterOS before 6.43.12 (stable) and 6.42.12 (long-term) is vulnerable to an intermediary vulnerability. The software will execute user defined network requests to both WAN and LAN clients. A remote unauthenticated attacker can use this vulnerability to bypass the router's firewall or for general network scanning activities. CVE ID : CVE-2019-3924	N/A	O-MIK-ROUT-030419/375
-----	------------	---	--	-----	-----------------------

netis-systems

wf2411_firmware

N/A	21-02-2019	9	On Netis WF2880 and WF2411	N/A	O-NET-
-----	------------	---	----------------------------	-----	--------

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.1.36123 devices, there is a stack-based buffer overflow that does not require authentication. This can cause denial of service (device restart) or remote code execution. This vulnerability can be triggered by a GET request with a long HTTP "Authorization: Basic" header that is mishandled by user_auth->user_ok in /bin/boa. CVE ID : CVE-2019-8985		WF24-030419/376
wf2880_firmware					
N/A	21-02-2019	9	On Netis WF2880 and WF2411 2.1.36123 devices, there is a stack-based buffer overflow that does not require authentication. This can cause denial of service (device restart) or remote code execution. This vulnerability can be triggered by a GET request with a long HTTP "Authorization: Basic" header that is mishandled by user_auth->user_ok in /bin/boa. CVE ID : CVE-2019-8985	N/A	O-NET-WF28-030419/377
Phoenixcontact					
axc_1050_firmware					
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive	N/A	O-PHO-AXC_-030419/378

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201							
ilc_131_eth/xc_firmware										
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201	N/A	O-PHO-ILC_-030419/379					
ilc_131_eth_firmware										
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201	N/A	O-PHO-ILC_-030419/380					
ilc_151_eth/xc_firmware										
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH,	N/A	O-PHO-ILC_-					
CV Scoring Scale (CVSS)										
0-1		1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201		030419/381					
ilc_151_eth_firmware										
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201	N/A	O-PHO-ILC_-030419/382					
ilc_171_eth_2tx_firmware										
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to	N/A	O-PHO-ILC_-030419/383					
CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traverse all directories. CVE ID : CVE-2019-9201		
ilc_191_eth_2tx_firmware					
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201	N/A	O-PHO-ILC_-030419/384
ilc_191_me/an_firmware					
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, ILC 151 ETH/XC, ILC 171 ETH 2TX, ILC 191 ETH 2TX, ILC 191 ME/AN, and AXC 1050 devices allow remote attackers to establish TCP sessions to port 1962 and obtain sensitive information or make changes, as demonstrated by using the Create Backup feature to traverse all directories. CVE ID : CVE-2019-9201	N/A	O-PHO-ILC_-030419/385
Redhat					
enterprise_linux_desktop					
N/A	19-02-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed	N/A	O-RED-ENTE-030419/386

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy. CVE ID : CVE-2019-5754		
N/A	19-02-2019	5.8	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. CVE ID : CVE-2019-5755	N/A	O-RED-ENTE-030419/387
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5756	N/A	O-RED-ENTE-030419/388
N/A	19-02-2019	6.8	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. CVE ID : CVE-2019-5757	N/A	O-RED-ENTE-030419/389
N/A	19-02-2019	6.8	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.	N/A	O-RED-ENTE-030419/390

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5758		
N/A	19-02-2019	6.8	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5759	N/A	O-RED-ENTE-030419/391
N/A	19-02-2019	6.8	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5760	N/A	O-RED-ENTE-030419/392
N/A	19-02-2019	6.8	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5761	N/A	O-RED-ENTE-030419/393
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5762	N/A	O-RED-ENTE-030419/394
N/A	19-02-2019	6.8	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81	N/A	O-RED-ENTE-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5763		030419/395
N/A	19-02-2019	6.8	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5764	N/A	O-RED-ENTE-030419/396
N/A	19-02-2019	4.3	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent. CVE ID : CVE-2019-5765	N/A	O-RED-ENTE-030419/397
N/A	19-02-2019	4.3	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2019-5766	N/A	O-RED-ENTE-030419/398
N/A	19-02-2019	4.3	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web	N/A	O-RED-ENTE-030419/399

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APIs via a crafted APK. CVE ID : CVE-2019-5767		
N/A	19-02-2019	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension. CVE ID : CVE-2019-5768	N/A	O-RED-ENTE-030419/400
N/A	19-02-2019	6.8	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5769	N/A	O-RED-ENTE-030419/401
N/A	19-02-2019	6.8	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. CVE ID : CVE-2019-5770	N/A	O-RED-ENTE-030419/402
N/A	19-02-2019	6.8	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2019-5771	N/A	O-RED-ENTE-030419/403
N/A	19-02-2019	6.8	Sharing of objects over calls into	N/A	O-RED-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2019-5772		ENTE-030419/404
N/A	19-02-2019	4.3	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. CVE ID : CVE-2019-5773	N/A	O-RED-ENTE-030419/405
N/A	19-02-2019	6.8	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file. CVE ID : CVE-2019-5774	N/A	O-RED-ENTE-030419/406
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5775	N/A	O-RED-ENTE-030419/407
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome	N/A	O-RED-ENTE-030419/408

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5776		
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5777	N/A	O-RED-ENTE-030419/409
N/A	19-02-2019	4.3	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. CVE ID : CVE-2019-5778	N/A	O-RED-ENTE-030419/410
N/A	19-02-2019	4.3	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2019-5779	N/A	O-RED-ENTE-030419/411
N/A	19-02-2019	4.6	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute	N/A	O-RED-ENTE-030419/412

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			JavaScript via Apple Events. CVE ID : CVE-2019-5780		
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5781	N/A	O-RED-ENTE-030419/413
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2019-5782	N/A	O-RED-ENTE-030419/414

enterprise_linux_server

N/A	19-02-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy. CVE ID : CVE-2019-5754	N/A	O-RED-ENTE-030419/415
N/A	19-02-2019	5.8	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. CVE ID : CVE-2019-5755	N/A	O-RED-ENTE-030419/416

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5756	N/A	O-RED-ENTE-030419/417
N/A	19-02-2019	6.8	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. CVE ID : CVE-2019-5757	N/A	O-RED-ENTE-030419/418
N/A	19-02-2019	6.8	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5758	N/A	O-RED-ENTE-030419/419
N/A	19-02-2019	6.8	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5759	N/A	O-RED-ENTE-030419/420
N/A	19-02-2019	6.8	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to	N/A	O-RED-ENTE-030419/421

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5760		
N/A	19-02-2019	6.8	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5761	N/A	O-RED-ENTE-030419/422
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5762	N/A	O-RED-ENTE-030419/423
N/A	19-02-2019	6.8	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5763	N/A	O-RED-ENTE-030419/424
N/A	19-02-2019	6.8	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5764	N/A	O-RED-ENTE-030419/425

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	4.3	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent. CVE ID : CVE-2019-5765	N/A	O-RED-ENTE-030419/426
N/A	19-02-2019	4.3	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2019-5766	N/A	O-RED-ENTE-030419/427
N/A	19-02-2019	4.3	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK. CVE ID : CVE-2019-5767	N/A	O-RED-ENTE-030419/428
N/A	19-02-2019	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension. CVE ID : CVE-2019-5768	N/A	O-RED-ENTE-030419/429
N/A	19-02-2019	6.8	Incorrect handling of invalid	N/A	O-RED-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5769		ENTE-030419/430
N/A	19-02-2019	6.8	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. CVE ID : CVE-2019-5770	N/A	O-RED-ENTE-030419/431
N/A	19-02-2019	6.8	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2019-5771	N/A	O-RED-ENTE-030419/432
N/A	19-02-2019	6.8	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2019-5772	N/A	O-RED-ENTE-030419/433
N/A	19-02-2019	4.3	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin	N/A	O-RED-ENTE-030419/434

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			policy via a crafted HTML page. CVE ID : CVE-2019-5773								
N/A	19-02-2019	6.8	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file. CVE ID : CVE-2019-5774	N/A	O-RED-ENTE-030419/435						
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5775	N/A	O-RED-ENTE-030419/436						
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5776	N/A	O-RED-ENTE-030419/437						
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5777	N/A	O-RED-ENTE-030419/438						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	19-02-2019	4.3	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. CVE ID : CVE-2019-5778	N/A	O-RED-ENTE-030419/439
N/A	19-02-2019	4.3	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2019-5779	N/A	O-RED-ENTE-030419/440
N/A	19-02-2019	4.6	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events. CVE ID : CVE-2019-5780	N/A	O-RED-ENTE-030419/441
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5781	N/A	O-RED-ENTE-030419/442
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81	N/A	O-RED-ENTE-030419/443

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2019-5782								
enterprise_linux_workstation											
N/A	19-02-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy. CVE ID : CVE-2019-5754	N/A	O-RED-ENTE-030419/444						
N/A	19-02-2019	5.8	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. CVE ID : CVE-2019-5755	N/A	O-RED-ENTE-030419/445						
N/A	19-02-2019	6.8	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5756	N/A	O-RED-ENTE-030419/446						
N/A	19-02-2019	6.8	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML	N/A	O-RED-ENTE-030419/447						
CV Scoring Scale (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.											

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. CVE ID : CVE-2019-5757		
N/A	19-02-2019	6.8	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5758	N/A	O-RED-ENTE-030419/448
N/A	19-02-2019	6.8	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2019-5759	N/A	O-RED-ENTE-030419/449
N/A	19-02-2019	6.8	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5760	N/A	O-RED-ENTE-030419/450
N/A	19-02-2019	6.8	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5761	N/A	O-RED-ENTE-030419/451
N/A	19-02-2019	6.8	Inappropriate memory	N/A	O-RED-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. CVE ID : CVE-2019-5762		ENTE-030419/452
N/A	19-02-2019	6.8	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5763	N/A	O-RED-ENTE-030419/453
N/A	19-02-2019	6.8	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5764	N/A	O-RED-ENTE-030419/454
N/A	19-02-2019	4.3	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent. CVE ID : CVE-2019-5765	N/A	O-RED-ENTE-030419/455
N/A	19-02-2019	4.3	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin	N/A	O-RED-ENTE-030419/456

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data via a crafted HTML page. CVE ID : CVE-2019-5766		
N/A	19-02-2019	4.3	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK. CVE ID : CVE-2019-5767	N/A	O-RED-ENTE-030419/457
N/A	19-02-2019	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension. CVE ID : CVE-2019-5768	N/A	O-RED-ENTE-030419/458
N/A	19-02-2019	6.8	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2019-5769	N/A	O-RED-ENTE-030419/459
N/A	19-02-2019	6.8	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.	N/A	O-RED-ENTE-030419/460

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-5770		
N/A	19-02-2019	6.8	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2019-5771	N/A	O-RED-ENTE-030419/461
N/A	19-02-2019	6.8	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. CVE ID : CVE-2019-5772	N/A	O-RED-ENTE-030419/462
N/A	19-02-2019	4.3	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. CVE ID : CVE-2019-5773	N/A	O-RED-ENTE-030419/463
N/A	19-02-2019	6.8	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file. CVE ID : CVE-2019-5774	N/A	O-RED-ENTE-030419/464
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in	N/A	O-RED-ENTE-

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5775		030419/465
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5776	N/A	O-RED-ENTE-030419/466
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5777	N/A	O-RED-ENTE-030419/467
N/A	19-02-2019	4.3	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension. CVE ID : CVE-2019-5778	N/A	O-RED-ENTE-030419/468
N/A	19-02-2019	4.3	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81	N/A	O-RED-ENTE-030419/469

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. CVE ID : CVE-2019-5779		
N/A	19-02-2019	4.6	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events. CVE ID : CVE-2019-5780	N/A	O-RED-ENTE-030419/470
N/A	19-02-2019	4.3	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name. CVE ID : CVE-2019-5781	N/A	O-RED-ENTE-030419/471
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. CVE ID : CVE-2019-5782	N/A	O-RED-ENTE-030419/472
enterprise_linux					
N/A	18-02-2019	7.2	In the Linux kernel through 4.20.11, af_alg_release() in crypto/af_alg.c neglects to set a NULL value for a certain structure member, which leads to a use-after-free in sockfs_setattr.	N/A	O-RED-ENTE-030419/473

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-8912		
Xiaomi					
mi_mix_2_firmware					
N/A	17-02-2019	4.9	On Xiaomi MIX 2 devices with the 4.4.78 kernel, a NULL pointer dereference in the ioctl interface of the device file /dev/elliptic1 or /dev/elliptic0 causes a system crash via IOCTL 0x4008c575 (aka decimal 1074316661). CVE ID : CVE-2019-8413	N/A	O-XIA-MI_M-030419/474

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