

## 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 Dat	e CVSS		Descrip	tion & C\	/E ID		F	Patch	NCIIPC ID	
				Applica	tion						
advanceman	1e										
advancecom	р										
N/A	27-02-2019	4.3	png_c advpr upon PNG s attem a buff is also read.	compresing has a encounties, which more that it is a heap	tering ar ch resul emcpy to s too sm	ex.cc in r overflo n invalid ts in an o write in nall. (The ouffer ov	nto	N/A	A	A-ADV ADVA- 03041	
antfin											
sofa-hessian											
N/A	27-02-2019	7.5	allow execu a craf object com.s nal.ob misha Gadge	s remot te arbit ted seri t becaus caucho.r sun.org.a ojects.XS andled, n	alized Ho e blackli aming.Q apache.x	ers to nmands vessian isting of Name and path.inte	nd	N//	A	A-ANT SOFA- 03041	
Appneta											
Tcpreplay											
N/A	16-02-2019	6.8			discover 3.1. A NU	red in LL point	ter	N/A	A	A-APP 03041	-TCPR- 9/3
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9	9-10
Vulnerability T	ype(s): CSRF- Cr Denial of Sen	-				-					n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			dereference occurred in the function get_layer4_v6() located at get.c. This can be triggered by sending a crafted pcap file to the tcpreplay-edit 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 get_ipv6_l4proto() located at get.c. This can be triggered by sending a crafted pcap file to the tcpreplay-edit 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 do_checksum in checksum.c. It can be triggered by sending a crafted pcap file to the tcpreplay-edit binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact.	N/A	A-APP-TCPR- 030419/5
ascellamobil	e		CVE ID : CVE-2019-8381		
musicloud					

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 Musicloud 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 curfolder (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_web	 site_script_pro	ject			
auction_web	site_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_comm	unicator				
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://d ownloads .avaya.co m/css/P8 /docume nts/1010 55661	A-AVA-ONE 030419/8

CV Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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::GetSampleIndexFor TimeStampMs() located in Core/Ap4Track.cpp. It can 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

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	•	Patch	NCIII	PC 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 possible have unspecified other impact.  CVE ID: CVE-2019-8382	ly			
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.ja.  CVE ID: CVE-2019-9142	N/	A	A-B3L- SYMP- 03041	
bagesoft							
bagecms							
N/A	17-02-2019	6.5	upload/protected/modules/acmini/views/post/index.php in BageCMS through 3.1.4 allows SQL Injection via the title or titleAlias parameter.		A	A-BAG BAGE- 03041	
			CVE ID : CVE-2019-8421				
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 the allows remote attackers to inject arbitrary web script or HTML via the opt[base][BG_SITE_NAME] parameter to the	A	A-BAI- 03041		
CV Scoring Sca (CVSS)	le <b>0-1</b>	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
<u> </u>	• • • •	_	uest Forgery; Dir. Trav Directory Trave			nformation	n; DoS-
	Denial of Service	; x55- Cr	oss Site Scripting; Sql- SQL Injection; N/	A- NOT A	рысаріе.		

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		F	Patch	NCIII	PC ID
			=reque	st URI.			:&c				
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						A	A-BAI- 03041	
bosch											
smart_camer	'a										
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				sirt .com isom SCH 201		A-BOS SMAR- 03041		
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				sirt .com isom SCH 201		A-BOS SMAR- 03041		
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-	.7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID			
			affected.)					
			CVE ID : CVE-2019-7729					
british_airwa	ays				·			
entertainme	nt_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			0.2.2.0.2.20.2, 7.0.2,					
	ccess_manager							
N/A	26-02-2019	6.4	An improper authentication vulnerability in CA Privileged Access Manager 3.x Web-UI jkmanager 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								

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
\/ulnorability/Typo/s\	CCDE C	acc Sita Ba	auget For	aona Dir '	Trav Dira	ctory Tra	orcali ile	fo Goin I	oformation	a. Dos

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.	N/A	A-CAB-CAB 030419/20
Cisco			CVE ID : CVE-2019-9064		
webex_meet	inge online				
webex_meet	ings_oninie		A vulnerability in the update		
N/A	28-02-2019	9	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

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_infras	tructure				
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

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
prime_collab	oration_assur	ance			
N/A	21-02-2019	6.4	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.  CVE ID: CVE-2019-1662	N/A	A-CIS-PRIM- 030419/23
unity_connec	ction				
N/A	21-02-2019	4.3	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	N/A	A-CIS-UNIT- 030419/24

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	1	Patch	NCII	PC ID
			attacker could expended attacker could expended link. A succould allow the attexecute arbitrary the context of the interface or access browser-based in Version 12.5 is after the context of the context of the interface or access browser-based in the context of the interface or access browser-based in the context of the interface or access browser-based in the context of the interface or access browser-based in the context of the context o					
cmseasy			0.515.0.52.203	1000				
cmseasy								
N/A	17-02-2019	4.3	In CmsEasy 7.0, the ckplayer.php  CVE ID : CVE-201	url paramete		A	A-CMSE- 03041	-
N/A	17-02-2019	4.3	In CmsEasy 7.0, the ckplayer.php parameter.  CVE ID: CVE-201	autoplay	a N/	A	A-CMS CMSE- 03041	-
cmswing								
cmswing								
N/A	17-02-2019	5	global.encryptPas bootstrap/global. 1.3.7 relies on mu operations for pa hashing. CVE ID : CVE-201	js in CMSWir Iltiple MD5 ssword	ng N/	A	A-CMS CMSW 03041	<i>7</i> _
cordaware								
bestinformed	d							
N/A	25-02-2019	4.6	The Scripting and functionality in Cobestinformed Mic	N/.	A	A-COF 03041	R-BEST- .9/28	
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-	.5 5-6	6-7	7-8	8-9	9-10
(CVSS)			uest Forgery; Dir. Trav.					
	• • • •	_	oss Site Scripting; Sql- S	<del>-</del>				

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.	N/A	A-COR-BEST- 030419/29
			CVE ID : CVE-2019-6266		
custom_t-shi	rt_ecommerce	_script	project		
custom_t-shi	rt_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=s ave&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

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	ID .		F	Patch	NCII	PC 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 Scan upload a uploads/direction being blocked Application Fexecute this fexecute this fexecute this fexecute the template, Template Main on New Template Main on New Template Main on New Template Main Mew Template Main Mew Template Main Mew Template Main Mew Template Main New Template Main New Template Main Mew Template Mew Mew Mew Mew Mew Mew Mew Mew Mew Me	ectory (wind by the Walle, via this teps: visite page, clic clicking conagement of a lichard to/index to/index	o the thout Veb and the sting the king on Defat, clicking e from x.php.	en e i ult	N/A	A	A-DEI DEDE 03041	-
deltaww						1				
screeneditor									T	
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.				N/A	A	A-DEI 03041	SCRE- .9/33
Drupal			CVE ID : CVE-2019-6547							
Drupal										
N/A	21-02-2019	6.8	Some field types do not properly sanitize data from nonform sources in Drupal 8.5.x			on-	ww	ps://w v.synol v.com/	A-DRU DRUP 03041	-
CV Scoring Sca (CVSS)	le 0-1 ype(s): CSRF- Cross	1-2 Site Reg	2-3 3-4	4-5	5-6	6-		7-8	8-9	9-10

			befor arbitr some affect follow site h REST modu in Dru REST 7. (No modu an up shoul updat advis	e 8.6.10 cary PHF cases. A ed by the ving con as the D ful Web ale enable and the enable enable enable enable enable enable enable at the date at the date at the cory if Second enable	This can code examined a code	of the s met: Toore (rest) allows ests, or the services (SON:AP) es or s in Drup 7 Services to require to the this in use.)	in he lales	adv Syn	irity/ isory/ ology_ 19_09		
Eclipse			<u> </u>								
wakaama  In Eclipse Wakaama (formerly liblwm2m) 1.0, core/er-coap-13/er-coap-13.c in lwm2mserver 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.  CVE ID: CVE-2019-9004							7.	N/A		A-ECL WAKA 03041	
CV Scoring Scal	e 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
etsi					
enterprise_tr	ansport_secui	rity			
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.	N/A	A-EXI-EXIV- 030419/38
			CVE ID : CVE-2019-9144		
F5					
big-ip_access	_policy_manag	ger			

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type/s): CSPE Cross Site Paguest Forgery: Dir Tray Directory Trayersal: ±Info Gain Information: DoS										

Vulnerability Type(s)	Pu	blish Date	cvss	Description & CVE ID					P	atch	NCI	PC ID
N/A	26-	02-2019	6.4	may r file w certif serve	estart a hen vali icates in r SSL pr			upp con arti	os://s port.f5. n/csp/ cle/K 16706	A-F5-1 03041		
N/A	26-	02-2019	4.3	and 1 config profil chose CBC c this n recov throu (MIT) attacl acces key it know	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.)						A-F5-1 03041	
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					upp con arti	os://s oort.f5. n/csp/ cle/K 02626	A-F5-1 03041	
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					upp con arti	os://s oort.f5. n/csp/ cle/K	A-F5-1 03041	
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6595	6	
big-ip_advan	ced_firewall_n	nanage	r		
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/45
big-ip_analyt	cics				

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

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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/48
big-ip_applic	ation_security	_mana			
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://s upport.f5. com/csp/	A-F5-BIG 030419/49

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCI	IPC ID
				serve	icates in r SSL pr I <b>D : CVE</b>	ofiles.				icle/K 16706		
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.)						ps://s port.f5. m/csp/ icle/K 06517	A-F5- 03041	
N/A	26-	02-2019	4.3	12.1.3 13.1.3 Multi not p zero l reass lead t	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.					ps://s port.f5. n/csp/ icle/K 02626	A-F5- 03041	
big-ip_domai	in_na	ame_syste	m									
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					upj cor art	ps://s port.f5. m/csp/ icle/K 16706	A-F5- 03041	
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6		-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://s upport.f5. com/csp/ article/K 1006517	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://s upport.f5. com/csp/ article/K 9102626	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://s upport.f5. com/csp/ article/K 5416706	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://s upport.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)	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/K 1006517 3	
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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/57
big-ip_fraud_	_protection_se	rvice			
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	A-F5-BIG 030419/59

CV Scoring Scale (CVSS)

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-

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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/60
big-ip_global	_ l_traffic_manag	ger			
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	A-F5-BIG 030419/62

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.	https://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/63
			CVE ID: CVE-2019-6594		
big-ip_link_c	ontroller				
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	A-F5-BIG 030419/65

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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/66
hig-in local	traffic_manage	r	CVE ID . CVE-2019-0394		
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	A-F5-BIG 030419/68

5-6 0-1 1-2 2-3 3-4 4-5 6-7 7-8 8-9 9-10 (CVSS) 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.

CV Scoring Scale

19 4.	.3	On BIO 12.1.3 13.1.1 Multi- not pr zero le	G-IP 11. .4-12.1. .1, and Path T(	5.1-11.6 3.7, 13.0 14.0.0-1 CP (MPT)	0.3.2, 0.0 HF1- 4.0.0.2,		:ps://s		
19 4.	.3	12.1.3 13.1.1 Multi- not pr zero le	.4-12.1. .1, and Path T( otect ag	.3.7, 13.0 14.0.0-1 CP (MPT	0.0 HF1- 4.0.0.2,		ps://s		
		circun	embly q o an infi nstance	ATA_FINueue, whinite loop	ultiple  Is in the nich can p in some	con	port.f5. m/csp/ cicle/K 02626	A-F5-I 03041	
nent_ma	anag	ger							
19 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			up coi art	ps://s port.f5. m/csp/ cicle/K 16706	A-F5-I 03041		
19 4.	ా	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				htti up con art 10	ps://s port.f5. m/csp/ cicle/K 06517	A-F5-I 03041	
19 4.	.3	On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-							
CV Scoring Scale (CVSS)         0-1         1-2         2-3         3-4         4-5         5-6         6-7         7-8         8-9         9-10									
)	1-2	1-2 Cross Site Req	CVE II  On BIO 12.1.3  1-2  2-3  Cross Site Request Forg	CVE ID : CVE On BIG-IP 11. 12.1.3.4-12.1. 1-2 2-3 3-4 Cross Site Request Forgery; Dir.	CVE ID : CVE-2019-6 On BIG-IP 11.5.1-11.6 12.1.3.4-12.1.3.7, 13.0  1-2 2-3 3-4 4-5	CVE ID : CVE-2019-6593  On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-  1-2 2-3 3-4 4-5 5-6  Cross Site Request Forgery; Dir. Trav Directory Travers	CVE ID : CVE-2019-6593  On BIG-IP 11.5.1-11.6.3.2, htt up:  1-2 2-3 3-4 4-5 5-6 6-7  Cross Site Request Forgery; Dir. Trav Directory Traversal; +In	CVE ID : CVE-2019-6593  On BIG-IP 11.5.1-11.6.3.2, 12.1.3.4-12.1.3.7, 13.0.0 HF1-  1-2  2-3  3-4  4-5  5-6  6-7  7-8	CVE ID : CVE-2019-6593  On BIG-IP 11.5.1-11.6.3.2, https://s upport.f5.  1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9  Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information

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/K 9102626 1	
big-ip_webac	ccelerator				
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://s upport.f5. com/csp/ article/K 5416706	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://s upport.f5. com/csp/ article/K 1006517	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://s upport.f5. com/csp/ article/K 9102626	A-F5-BIG 030419/75

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.	1	
			CVE ID : CVE-2019-6594		
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.	N/A	A-FEI-FEIF- 030419/76
			CVE ID : CVE-2019-8412		
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.	N/A	A-FIL-FILE- 030419/77
			CVE ID : CVE-2019-8904		
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.	N/A	A-FIL-FILE- 030419/78
			CVE ID : CVE-2019-8905		
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	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
100050										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	)	Patch	NCIIPC ID
			memcpy is misused.			
			CVE ID: CVE-2019-8906	6		
N/A	18-02-2019	6.8	do_core_note in readelf.c libmagic.a in file 5.35 allo remote attackers to cause 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 In when the order_by or groparameter can be control  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 pdfimages 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 libiberty, as distributed in		N/A	A-GNU- BINU-
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5	5-6 6-	·7 7-8	8-9 9-10
(CVSS)  Vulnerability T	ype(s): CSRF- Cross	Site Req	uest Forgery; Dir. Trav Directory oss Site Scripting; Sql- SQL Injecti	y Traversal	; +Info- Gain Ir	

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.		030419/83
			CVE ID : CVE-2019-9070		
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.	N/A	A-GNU- BINU- 030419/84
			CVE ID : CVE-2019-9071		
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.	N/A	A-GNU- BINU- 030419/85
			CVE ID : CVE-2019-9072		
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

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_arma p in archive64.c.	N/A	A-GNU- BINU- 030419/88
			CVE ID : CVE-2019-9075		
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.	N/A	A-GNU- BINU- 030419/89
			CVE ID : CVE-2019-9076		
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.	N/A	A-GNU- BINU- 030419/90
			CVE ID : CVE-2019-9077		
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

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-G00- CHRO- 030419/94

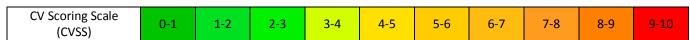
Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID				ı	Patch	NCII	PC ID	
			CVE ID	: CVE-	2019-5	754					
N/A	19-02-2019	5.8	Incorrect zero in Varior to remote arbitrar crafted CVE ID	V8 in 0 72.0.3 attack ry reac HTML	Google ( 3626.81 ter to pe l/write page.	N/A	A	A-GOO- CHRO- 030419/95			
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						A	A-G00- 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	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-G00- 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	A-GOO- CHRO- 030419/99	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE	Р	Patch		PC ID	
			remote attacker to potentially perform a sandbox escape via a crafted HTML page.						
			CVE ID : CVE						
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				1	A-G00- CHRO- 030419/100	
N/A	19-02-2019	6.8	Incorrect objection management Google Chron 72.0.3626.81 attacker to possible heap corrupt HTML page.  CVE ID: CVE	N/A	Δ	A-G00- 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				1	A-G00- 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				Λ	A-G00- CHRO- 030419/103	
CV Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish D	ate	cvss		Descrip	tion & C\	/E ID		Patch		NCII	PC ID		
N/A	19-02-20	)19	6.8	in We prior remo explo crafte	ebRTC in to 72.0. te attack it heap o		Chrome allowed tentially on via a	e da	N/A	A	A-GOC CHRO- 03041			
				_		-2019-5								
N/A	19-02-20	)19	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.						A	A-GOO- CHRO- 030419/105			
				CVE ID : CVE-2019-5765										
N/A	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.								N/A		A-G00- CHRO- 030419/106			
				<b>CVE ID : CVE-2019-5766</b>										
N/A	19-02-20	)19	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.					N/A		A-G00- CHRO- 030419/107			
				CVE I	D : CVE	-2019-5	767							
N/A	19-02-20	)19	4.3	DevTools API not correctly gating on extension capability in DevTools in Google Chrome					N/A		A-G00- CHRO- 030419/108			
CV Scoring Scale (CVSS)		1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10			

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID					atch	NCII	PC ID
			prior to 72.0 an attacker v user to insta extension to crafted Chro							
			CVE ID : CVI	E-2019-5	768					
N/A	19-02-2019	6.8	end character front render Google Chro 72.0.3626.83 attacker to p	correct handling of invalid and character position when ont rendering in Blink in pogle Chrome prior to 2.0.3626.81 allowed a remote tacker to potentially exploit eap corruption via a crafted TML page.					A-GOO- CHRO- 030419/109	
			CVE ID : CVI	E-2019-5						
N/A	19-02-2019	6.8	Insufficient in WebGL in Go to 72.0.3626 remote attact out of bound a crafted HT CVE ID : CVI	N/A	Α	A-GOC CHRO- 03041				
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					A	A-G00- 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.					A	A-G00- CHRO- 030419/112	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4	4-5	5-6	6	-7	7-8	8-9	9-10

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-G00- 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-G00- 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-G00- 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-G00- CHRO- 030419/116

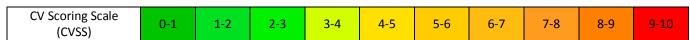


Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	otion & C\	/E ID		ı	Patch	NCII	PC ID
N/A	19-	02-2019	4.3	confu Omni prior remo conte bar)	rect han isable ch ibox in G to 72.0. te attacl ents of th	laracter Google Cl 3626.81 Ker to sp ne Omnil	in nrome allowed oof the pox (UR) nain nan	L	N/	A	A-GOC CHRO- 03041	
N/A	19-	02-2019	4.3	A mis speci reque Goog 72.0 attack to ins to by check crafte	issing case for handling cial schemes in permission uest checks in Extensions in gle Chrome prior to 0.3626.81 allowed an cker who convinced a user astall a malicious extension ypass extension permission cks for privileged pages via a ted Chrome Extension.			ng case for handling schemes in permission checks in Extensions in Chrome prior to 26.81 allowed an who convinced a user a malicious extension for privileged pages via a Chrome Extension.				)- - 9/118
N/A	19-	02-2019	4.3	Servi Chronallow bypas via a	ceWorkome prior yed a ren ss naviga crafted l	policy validation in ker in Google or to 72.0.3626.81 smote attacker to gation restrictions HTML page.				A	A-GOC CHRO- 03041	-
N/A	19-	02-2019	4.6	can b in Go prior local JavaS	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			ts	N/	A	A-GOC CHRO- 03041	•
N/A	19-	02-2019	4.3	Incor confu	rect han Isable ch	dling of aracter	a in		N/	A	A-G00- CHR0- 030419/12	
CV Scoring Sca (CVSS)	ale	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

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-G00- 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-G00- CHRO- 030419/123
Hdfgroup					
Hdf5					
N/A	17-02-2019	4.3	A buffer overflow in H50_layout_encode in H50layout.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 Sc	()-	·1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS)											

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.		030419/125
			CVE ID : CVE-2019-8397		
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_pro	oject				
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 URI.  CVE ID: CVE-2019-8407	N/A	A-HON- HONG- 030419/129



Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & C\	/E ID		Pa	atch	NCII	PC ID
hornerauton	nation									
cscape										
N/A	28-02-2019	6.8	Cscape, 9.80 simproper inp vulnerability by processing POC files. This attacker to reinformation	ut valida may be g special s may al ad confi and remo rary cod	ation exploite ly crafte low an dential otely e.	d d	N/A		A-HOI CSCA- 03041	R- 9/130
hotels_serve	r_project									
hotels_serve	r									
N/A	17-02-2019	7.5	Hotels_Server 05 has SQL In because the controller/ap telephone pa mishandled. CVE ID : CVE	ijection v i/login.j rameter	via the A php is	\PI	N/A		A-HO7E HOTE 03041	
hsycms	<u>'</u>									
hsycms										
N/A	25-02-2019	4.3	An issue was Hsycms V1.1. vulnerability to the /book CVE ID : CVE	There is via the r	s an XSS name fie		N/A			-HSYC- 9/132
IBM										
bigfix_platfo	rm									
N/A	27-02-2019	5	IBM BigFix Pl could allow a the relay rem information a and fixlets de	n attack otely an ibout the	er to quo d gather e update	ery	N/A			-BIGF- 9/133
CV Scoring Sca	le <b>0-1</b>	1-2	2-3 3-4	4-5	5-6	6-7	7	7-8	8-9	9-10
(CVSS)  Vulnerability T	ype(s): CSRF- Cross	Site Req		Trav Dire	ectory Trav	versal;	+Info	o- Gain lı		

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 URI.  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 URI.	N/A	A-IND-INDE- 030419/135
			CVE ID : CVE-2019-8954		
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://w ww.intel.c om/conte nt/www/ us/en/se curity- center/ad visory/IN TEL-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)	Publi	sh Date	cvss		Descrip	tion & C\	/E ID		F	atch	NCI	IPC ID
									ml			
openvino												
N/A	18-02	2-2019	2.1	Intel( R3 an allow poten disclo	R) Open d before a privil- itially er osure via	VINO(T e for Lin eged use	er to ormatio	3	www om nt/ us/ cur cen visc TEI	os://w cintel.c /conte www/ en/se ity- ter/ad ory/IN SA- 222.ht		-OPEN- 19/137
J2store												
J2store												
N/A	26-02	2-2019	7.5	the J2 3.3.7 attack SQL c	Store ploon for Joon kers to e omman ict_optic	ugin 3.x ıla! allov	ws remo arbitrary e ameter.	te	N/A	A	A-J2S- 03041	-J2ST- 19/138
Jamf												
self_service												
N/A	25-02	2-2019	7.9	man- obtain the "p featur "/App al app/(	in-the-ment a root oublish I re to insolication.  Contents the TCF	niddle at shell by Bash she ert s/Utiliti		to ing s" nin	N/A	A	_	I-SELF- 19/139
Jenkins												
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
Vulnerability T		SRF- Cross I of Service									ntormatio	on; DoS-

Vulnerability Type(s)	Pub	olish Date	cvss		Descrip	tion & C\	/E ID		F	Patch	NCII	IPC ID
script_securi	ty											
N/A	20-0	)2-2019	6.5	exists Plugit Reject r.java Overa provi HTTF in ark	s in Jenks n 1.52 and tASTTra that allowed all/Read de a Gro endpoi onkins m	ins Scrip nd earlie insforms ows atta permiss ovy scri nt that c ode exec aster JV	sCustom ckers wi sion to pt to an an resul cution or M.	ty ize ith t	nki ecu dvi 019	ps://je ns.io/s irity/a sory/2 9-02- /#SEC ITY-		-SCRI- 19/140
aland farm du				CVE	D: CVE	-2019-1	003024	<u> </u>				
cloud_foundr		02-2019	4	informin Jene 2.3.1 Abstraction with connection URL user through the capture Jenkin	mation values Cloud and earl actCloud rijava the Overall/ect to an assing attentials II gh another ing creas.	ud Foundrier in dFoundrat allows Read actacker acker-sposobtain her metl	ility exisodry Plug ryPushDess attacked cess to r-specificed ned	gin esc ers ed	nki ecu dvi 019	ps://je ns.io/s irity/a sory/2 9-02- /#SEC ITY-		-CLOU- 19/141
mattermost												
N/A	20-(	)2-2019	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				nki ecu dvi 019	ps://je ns.io/s nrity/a sory/2 9-02- /#SEC ITY-	A-JEN MATT 03041		
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
Vulnerability Ty		ial of Service	_				_				irormatic	או; שמן; טס

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		F	Patch	NCII	PC ID
			serve mess	r and ro	om and						
octonucdonle	287		CVE	D : CVE	-2019-1	.003026	)				
octopusdeple	D <b>y</b>		A cer	ver-side	request	forgery					
N/A	20-02-2019	4	vulne Octor earlie Octor allow Overa have attack obtain if succerror	rability busDeplo or in busDeplo s attack all/Read Jenkins ker-spec n the HT cessful, messag	exists in by Plugin ers with permise connect ified UR TP resp and exce e otherv	Jenkins on 1.8.1 and sion to to an L and onse coor	nd at	nki ecu dvi 019	ps://je ns.io/s nrity/a sory/2 9-02- /#SEC ITY-		-OCTO- 9/143
jms_messagi	ng										
N/A	20-02-2019	4	vulne JMS M earlie SSLCe thod. Userr d.java Overa have endpe	rability Messagin er in ertificate iava, nameAut that all All/Read Jenkins oint.	exists in g Plugin eAuthen thenticat ows atta permiss connect	forgery Jenkins 1.1.1 ar tication! tionMeth ackers w sion to to a JMS	md Me ho rith	nki ecu dvi 019	ps://je ns.io/s nrity/a sory/2 9-02- /#SEC ITY-	A-JEN 03041	-JMS .9/144
jtbc											
jtbc_php											
N/A	17-02-2019	5		. ,	0.1.8 alle Upload			N/A	A	A-JTB 03041	-JTBC- .9/145
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
vuinerability Ty	ype(s): CSRF- Cros Denial of Servic	_				_				nformatio	n; D0S-

Vulnerability Type(s)	Publish Dat	e CVSS	Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
			console/#/co .php?type=lis demonstrated	t URI, as d by a .pl	hp file.	ge				
kohanafram	arrault		CVE ID : CVE	-2019-8	3433					
kohana	ework									
Kullalla	T		Vacayan thro	ugh 2.2	0 and		I			
N/A	21-02-2019	7.5	Koseven thro Kohana throu Injection whe parameter ca CVE ID : CVE	igh 3.3.6 on the or n be con	, has SQI der_by() trolled.		N/A	A	A-KOI KOHA 03042	
koseven	<u> </u>									
koseven										
N/A	21-02-2019	7.5	Koseven through Kohana through Injection who parameter ca	igh 3.3.6 on the or n be con	, has SQI der_by() trolled.		N/A	A		S-KOSE- 19/147
Laravel										
framework										
N/A	24-02-2019	7.5	The Illuminate Laravel Frame describilization that can lead execution if the controllable,destruct meaningCompandingCompand CVE ID : CVE	ework 5 on vulner to remothe contered technology the contered technology the contered to the content	a.7.x has a rability te code nt is to the the ass in p.	a	N/A	A	A-LAF FRAM 03042	
Libming										
ming										
N/A	24-02-2019	9 6.8	Ming (aka lib	ming) 0.	4.8 has a	l	N/A	A	A-LIB	-MING-
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4	4-5	5-6		-7	7-8	8-9	9-10
Vulnerability T		-	uest Forgery; Dir. oss Site Scripting;		_					on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVE ID		Patch	NCIII	PC ID
			function getS	dereference in the ile in libutil.a.	the		03041	9/149
			CVE ID : CVE	-2019-9113				
N/A	24-02-2019	6.8	out of bounds vulnerability	in the function the decompile	l N	I/A	A-LIB- 03041	
Live555								
streaming_m	edia							
N/A	27-02-2019	7.5	malformed he invalid memo	ory access in the zationHeader	e	I/A	A-LIV- 03041	
			CVE ID : CVE	-2019-9215				
maccms								
maccms				W W W W W W W W W W W W W W W W W W W				
N/A	27-02-2019	4.3	inc/config/ca parameter be template/pac .html mishand parameter, an a/tpl/module	ody/html/vod_ dles the keywo nd e/db.php only ame parameter	type rds N	I/A	A-MAC MACC- 03041	
matio_projec	t							
matio								
N/A	23-02-2019	5		discovered in matio (aka MA'		I/A	A-MATI-	`
CV Scoring Sca	le 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS)  Vulnerability Ty	ype(s): CSRF- Cross							
	• • • •	_		Sql- SQL Injection;				

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.		030419/153
			CVE ID: CVE-2019-9026		
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.	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 Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish	Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
				CVE I	D : CVE	-2019-9	030					
N/A	23-02-2	2019	5	libma File I, a NUI the fu mat.c	ntio.a in 1 /O Libra LL point unction I	discover matio (a ry) 1.5.1 er derefe Mat_Varl	ka MAT 13. Ther erence in Free() in	e is n	N/A	A	A-MA MATI 03042	
				CVE I	D : CVE	-2019-9	031					
N/A	23-02-2	2019	5	libma File I, an ou causi	ntio.a in 1 /O Libra nt-of-boung a SEC	discover matio (a ry) 1.5.1 inds wri W in the ) in mat	ka MAT 13. Therete probl function	e is em	N/A	Α	A-MA MATI 03042	
				CVE I	D : CVE	-2019-9	032					
N/A	23-02-2	2019	6.4	libma File I, a stac for th featu	ntio.a in note.  Ck-based ne "Rank re in the NextCell	discover matio (a ry) 1.5.1 buffer o and Din function () in ma	ka MAT .3. Therever-rea nension' n t5.c.	e is d	N/A	A	A-MA MATI 03042	
				CVE	D : CVE	-2019-9	033					
N/A	23-02-2	2019	6.4	libma File I, a stac for a	ntio.a in 1 /O Libra ck-based memcpy	discover matio (a ry) 1.5.1 buffer o in the fo () in ma	ka MAT 13. Ther over-rea unction		N/A	A	A-MA MATI 03042	
				CVE I	D : CVE	-2019-9	034					
N/A	23-02-2	2019	6.4	libma File I, a stac in the	atio.a in 1 /O Libra ck-based e functio	discover matio (a ry) 1.5.1 buffer c n ictField(	ka MAT 13. Ther over-rea	e is	N/A	A	A-MA MATI 03042	
CV Scoring Sca	ıle 0-	1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10
(CVSS)  Vulnerability T												

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.	N/A	A-MAT- MATI- 030419/163
			CVE ID : CVE-2019-9036		
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.	N/A	A-MAT- MATI- 030419/164
			CVE ID: CVE-2019-9037		
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.	N/A	A-MAT- MATI- 030419/165
			CVE ID : CVE-2019-9038		
Mcafee					
endpoint_sec	curity				
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.c om/corpo rate/inde x?page=c ontent&id =SB1025 4	A-MCA- ENDP- 030419/166

CV Scoring Scale	0_1	1_2	2_2	2_/1	4-5	5-6	6-7	7₋0	Q_Q	0-10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	6-7	7-8	8-3	3-10

Vulnerability Type(s)	Pul	blish Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	PC ID
Agent												
N/A	28-	02-2019	5	Lengt (MA) unaut poten servic UDP p	th Value 5.x allow thentica tially ca ce via sp backets.	ws remo ted user use a de	ee Agent te s to mial of y crafted		c.m om rate x?p ont	os://k cafee.c /corpo e/inde age=c ent&id 31027	A-MCA AGEN 03041	
N/A	28-	02-2019	4.3	vulne (which McAforemon to according remon via re enabl	rability th is disa ee Agent te unaut eess sens mote lo ed.	abled by t (MA) 5 thenticat	ote logging default)  .x allowsted users  formations  hen it is	in S	c.m om rate x?p ont	os://k cafee.c /corpo e/inde age=c ent&id 31027	A-MCA AGEN 03041	
Microfocus												
filr												
N/A	20-	02-2019	4	the woof Midremo as a lodown the Fivulne of Film	eb applice of Focus to attack ow privious artification ar	ication cases Filr 3.3 ser author lege use oitrary fire.	les from Ill versio curity	nt a d	N/A	A		-FILR- 9/169
N/A	20-	02-2019	7.2	vulne comp 3.0 al	rability onent o lows a lo	ocal atta	mtd Focus Fil		N/A	A		FILR- 9/170
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8	8-9	9-10
Vulnerability T		: CSRF- Cross ial of Service	_				=				ntormatio	on; DoS-

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			GVEID. GVE 2017 3473		
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∾=list&menuid= 28∾=add&menuid=29 URI.	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
(6,033)										

Vulnerability Type(s)	Pul	blish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCII	PC ID					
Snapdrive																	
N/A	27-	02-2019	4.3	fatal calls (once once Open differ appli recei comp recei the a differ way t remo to a p be us order "non- must ciphe imple comr Also SSL_s proto (appl but s Open 1.0.2	application protocol SSL_shure to send to receive SSL can rently to cation if wed with pplication rently bathat is dependently being the application of the application of the applications of the app	error and tdown() a close_ve one) the calling a 0 byte invalid if a 0 byte an invalid in an invalid inv	twice notify, a chen lang record padding te record lid MAC behaves hat in a ce to the samount at could ta. In exploitable resuites ed mised ertain ersuites. In curred not do the ce ted 1.0.2	and is d is l ts l	sl.c	ps://w v.opens org/ne /secad 201902 txt	A-NET SNAP- 03041						
element_soft	ware	e															
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				fatal protocol error and then calls SSL_shutdown() twice			fatal protocol error and then calls SSL_shutdown() twice			ww sl.c	ps://w v.opens org/ne /secad	A-NET ELEM- 03041	•
CV Scoring Sca	ıle	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10					

2-3 (CVSS) 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	Descri	ption & CV	E ID		P	atch	NCII	PC ID
			once to receioned openSSL can application in the application of the ap	respond the calling of a 0 byte of an invalid price on the cased on the etectable of the cased o	record is padding a record in the amount at could a. In ploitable uites d ised rtain reuites. ust call even if a urred ot do the Fixed in the discount and the fixed in the discount at the fixed in the discount at the discount at the fixed in the discount at the discount	is If	v/2 26.1	01902 txt		
N/A	23-02-2019	6.8	An issue was Binutils 2.32 buffer overfloprocess_mips readelf.c via option section	. It is a hea ow in s_specific a malform on.	ap-based in ned MIP:	d	N/A	A	A-NET ELEM- 03041	•
hyper_conve	rged_infrastru	cture	10				1		A NIE	
N/A	27-02-2019	4.3	lf an applicat fatal protoco				•	os://w v.opens	A-NET HYPE-	
CV Scoring Sca (CVSS)	le 0-1 ype(s): CSRF- Cross	1-2 Site Reg	2-3 3-4	4-5	5-6	6-		7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		P	Patch	NCII	PC ID
			(once once to OpenS differed application received the application of t	to send o received SL can ently to ation if ed with plication ently banat is determined to defor this extitched for this extitute and the extitute of the e	re one) to respond the calling a 0 byte invalid if a 0 byte an invalid if a 0 be expected by the catter one of contraction in an () twice anyway)	notify, a chen ing record in padding te record lid MAC. behaves hat in a e to the s amoun lat could ta. In eploitable suites ed mised ertain ersuites. nust call e even if curred not do the ted 1.0.2	is g d is . If e	ws	rg/ne /secad 201902 txt	03041	9/176
oncommand_	_unified_mana	ger									
N/A	27-02-2019	4.3	fatal p calls S (once once t OpenS differe	rotocol SL_shut to send o receiv SSL can	error and the color of the color of the color of the calli	twice notify, a hen l	nd	ww sl.o ws,	ps://w v.opens rg/ne /secad 201902 txt	A-NET ONCO 03041	
CV Scoring Sca (CVSS) Vulnerability Ty	/pe(s): CSRF- Cross	-	_	-		_		; +Inf		8-9 nformatio	9-10 n; DoS-
•	Denial of Service	-	_	-		_					

Vulnerability Type(s)	Pul	blish Date	cvss		Descrip	otion & C\	/E ID		ı	Patch	NCI	IPC ID
				compreceive the application of the application of the commust cipher implements of the communication of the communica	eared to ved with oplication and to de te peer, adding ed to de for this estitched be in us reuites and the applications of the collections of the	invalid if a 0 byte an invalid on then be seed on the crypt date to be expected in the crypt date of t	te recordid MAC behaves hat in a to the samound ta. In aploitable suites ed ertain ersuites. In a to the even if curred not do the ted 1.0.2	d is . If . ts . e				
oncommand.	wor	kflow_a	utomati	on								
N/A	27-	02-2019	4.3	fatal j calls s (once once Open differ applic receiv comp receiv the aj differ	protocolossL_shue to receive SSL can rently to cation if wed with ared to wed with polication to rently barently barentl	ion enco error and tdown() a close_ve one) the respond the calling a 0 byte a invalid if a 0 byte a an invalid on then the sed on the	nd then twice notify, a hen ng record padding te record lid MAC behaves hat in a	and is d is	ww sl.c ws v/2	ps://w v.opens org/ne /secad 201902 txt	A-NEZ ONCO 03042	
CV Scoring Sca (CVSS) Vulnerability Ty	ype(s)	0-1 : CSRF- Cro ial of Servi	-				_		; +In		8-9 nformation	9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID		Patch	NCII	PC ID
			remote peer, then this amount 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 protocol error has occurred (applications should not do th but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2 1.0.2q).  CVE ID: CVE-2019-1559	a is			
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, at once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record i received with invalid padding compared to if a 0 byte record received with an invalid MAC. the application then behaves differently based on that in a way that is detectable to the remote peer, then this amount 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	nd s lis If	https://w ww.opens sl.org/ne ws/secad v/201902 26.txt	A-NET ONTA- 03041	-
CV Scoring Sca (CVSS)	o-1	1-2	<b>2-3</b> 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Travoss Site Scripting; Sql- SQL Injection; N,			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVE ID		Patch	NCI	IPC ID
			implementation commonly us Also the appl SSL_shutdow protocol erro (applications but some do a	are optimised ions of certain sed ciphersuites. ication must call in () twice even if or has occurred should not do thanyway). Fixed in 2r (Affected 1.0.2	fa nis n			
ontap_select	_deploy_admii	istrati	on_utility					
N/A	27-02-2019	4.3	fatal protocol calls SSL_shu (once to send once to receive OpenSSL can differently to application if received with compared to received with the application differently baway that is deremote peer, to a padding be used to de order for this "non-stitched must be in us ciphersuites a implementation commonly us Also the appl SSL_shutdow	respond the calling a 0 byte record invalid padding if a 0 byte record an invalid MAC on then behaves used on that in a etectable to the then this amoun oracle that could crypt data. In to be exploitable " ciphersuites	is g d is . If	https://w ww.open sl.org/ne ws/secad v/201902 26.txt	A-NETONTA	
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
				Trav Directory Trav Sql- SQL Injection; N				n; DoS-

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_sn	ni-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	https://w ww.opens sl.org/ne ws/secad v/201902 26.txt	A-NET- SANT- 030419/182

CV Scoring Scale (CVSS)

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-

			Also t								
			proto (appli but so Opens 1.0.20	hutdown col error cations ome do a SSL 1.0.2	cation n n() twice r has occ should n nyway) 2r (Affec	a is 1					
steelstore_clo	oud_integrated	d_stora	ge								
N/A	27-02-2019	4.3	fatal process calls S (once once to Open S differed application of the	corotocol SSL_shut to send to receive SSL can ently to cation if yed with a polication ently bath at is determined to deed to	error and down() a close_re one) the calling a 0 byte invalid and invalid and invalid and invalid and then this bracle the crypt date to be experied on sof common of	twice notify, a hen I ng record i padding te record id MAC. Dehaves hat in a e to the samoun at could ta. In eploitable suites ed mised ertain ersuites. In the suites ed ertain ersuites. In the suites ed even if e even if	nd s lis ts a is	ww sl.o ws,	ps://w v.opens rg/ne /secad 201902 txt		-STEE- 9/183
CV Scoring Scale (CVSS)	e <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			1.0.2q).  CVE ID : CVE-2019-1559  In the GNU C Library (aka glibc		
N/A	25-02-2019	7.5	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.	N/A	A-NET-STEE- 030419/184
			CVE ID : CVE-2019-9169		
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://w ww.opens sl.org/ne ws/secad v/201902 26.txt	A-NET- STOR- 030419/185

5-6 0-1 1-2 2-3 3-4 4-5 6-7 7-8 8-9 9-10 (CVSS) 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.

CV Scoring Scale

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	PC ID
				but so Open 1.0.20	ome do a SSL 1.0.: q).	should in should	. Fixed i	n				
element_soft	war	e_manage	ment									
N/A	23-	02-2019	6.8	libibe Binut buffe d_exp dema recur	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	A-NET ELEM 03041	
N/A	23-	02-2019	4.3	libibe Binut consu d_cou dema recur	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 cpdemangle.c after many recursive calls.					A	A-NET ELEM 03041	
				CVE I	D : CVE	-2019-9	071					
N/A	23-	02-2019	4.3	Binar librar distri It is a mem	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.					A	A-NET ELEM 03041	
				_								
N/A	23-	02-2019	4.3	Binar librar distri It is a	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	Α	A-NET ELEM 03041	
CV Scoring Sca (CVSS)		0-1	1-2							8-9	9-10	
Vulnerability Ty		: CSRF- Cross nial of Service	-				_					n; DoS-

Vulnerability Type(s)	Publish Da	ate CVSS		Descrip	otion & C\	/E ID		P	atch	NCII	PC ID				
			elf.c.	elf_slurp I <b>D : CVE</b>			in								
N/A	23-02-20	19 4.3	Binar librar distri It is a leadir in lib pex6- pei-x	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					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.				A-NET ELEM 03041		
N/A	23-02-20	19 6.8	Binar librar distri It is a overf _bfd_ p in a	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_arma p in archive64.c.				N/A		A-NET ELEM 03041					
N/A	23-02-20	19 4.3	Binar librar distri It is a mem elf_re	CVE ID: CVE-2019-9075  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	<b>L</b>	A-NET ELEM 03041					
cloud_backuj	p	•													
N/A	25-02-20	7.5	or lib proce posix	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heapbased buffer over-read via an						A-NET CLOU- 03041					
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10				
Vulnerability Ty			_		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					ı	Patch	NCII	IPC ID
			attempt	ted cas	se-insen	sitive					
			regular	-expre	ession m	atch.					
			CVE ID	: CVE	2019-9	169					
clustered_da	ta_ontap										
N/A	27-02-2019	5	prior to 9.3P7 a vulnera sensitiv unautho	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		ecu tap /ac /nt 201	ps://s prity.ne p.com dvisory cap- 19022		Γ-CLUS 19/194		
Nvidia			CVEID	: CVE-	-2019-5	491		7-0	,001/		
gpu_driver	I		NUUDIA	TA7: 1	CDI	ID: 1				I	
N/A	27-02-2019	7.2	driver of in the 3 which to softwar does no This believecution	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.			y n	vid hel /ap we	ps://n ia.cust p.com op/ans rs/det /a_id/4		-GPU 19/195
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			xt ich ng ct cly the	vid hel /ap we	ps://n ia.cust p.com op/ans rs/det /a_id/4		-GPU 19/196	
CV Scoring Sca	le a	1.2						_	7.0	0.0	
(CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Vulnerability Type(s)	Pul	blish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCII	PC ID
				escala	ation of	of servi privilege -2019-5	es.					
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				vid hel /ap we	ps://n ia.cust p.com op/ans rs/det /a_id/4		-GPU 9/197	
N/A	27-	02-2019	7.2	Drive in the (nvld Dxgk) l in w deref expec which service privil	NVIDIA Windows GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiSubmitCommandVirtua l 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.				vid hel /ap we	ps://n ia.cust p.com op/ans rs/det /a_id/4 2		-GPU 9/198
N/A	27-	02-2019	7.2	CVE ID: CVE-2019-5668  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			y it ry	vid hel /ap we	ps://n ia.cust p.com op/ans rs/det /a_id/4		-GPU .9/199	
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
Vulnerability Ty		: CSRF- Cross ial of Service	_				-				ntormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	otion & CVI	E ID		P	atch	NCII	PC ID
			the buffer, when denial of serve privileges.  CVE ID : CVE	vice or esc	alation	of				
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				vidi help /ap wer	os://n a.cust o.com p/ans rs/det a_id/4		-GPU 9/200
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				vidi help /ap wer	os://n a.cust o.com p/ans rs/det a_id/4		-GPU 9/201
octopus										
octopus_dep	loy					1				
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			<b>:</b>	N/A	Δ	A-OCT OCTO- 03041	
CV Scoring Sca (CVSS)	le 0-1 ype(s): CSRF- Cross	1-2 Site Reg	2-3 3-4 uest Forgery: Dir.	4-5 Trav Direc	5-6	6-7		7-8 o- Gain Ir	8-9	9-10 n: DoS-

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_p	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_scri	nt proje			
	ordering_scri	<u> </u>			
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
opensourcel	oms				
open_source	_background_	manag	ement_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/invokefunction&function=call_user_func_array&vars[0]=system&	;	A-OPE- OPEN- 030419/206
CV Scoring Sca	ale 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.

(CVSS)

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	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://w ww.opens sl.org/ne ws/secad v/201902 26.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)	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-com	n				
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				I.	
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				<u> </u>	

	CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
- 1	Male and little Towards CODE Consection Demonstration District District Demonstration Dec								- D-C		

Vulnerability Type(s)	Publish Date   CVSS   Description & CVE ID		Patch	NCIIPC ID	
Pbootcms					
N/A 17-02-201		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_ele ment.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)	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	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/regco mp.c, ext/mbstring/oniguruma/regex ec.c, ext/mbstring/oniguruma/regpa 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	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)	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	N/A	A-PHP-PHP- 030419/217				
php_appoint	ment_booking	_script	_project					
php_appoint	ment_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			
, ,			CVE ID : CVE-2019-9000					
phpmywind								
phpmywind		_						
N/A 17-02-2019 3.5		3.5	admin/default.php in PHPMyWind v5.5 has XSS via an HTTP Host header.  CVE ID: CVE-2019-8435	n N/A	A-PHP- PHPM- 030419/219			
nivolino								
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/configsetup.php allows remote attackers to execute arbitrary PHP code via the database_host	N/A	A-PIX-BUGS- 030419/220				
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6  uest Forgery; Dir. Trav Directory Traver	6-7 7-8	8-9 9-10			

Vulnerability Type(s) Publish Date		cvss	Description & CVE ID	Patch	NCIIPC ID
			remains present in its original directory after installation is		
			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_dele te&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_del ete&var1= URI.	N/A	A-PLU-PLUC- 030419/222
			CVE ID : CVE-2019-9049		
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.	N/A	A-PLU-PLUC- 030419/223
			CVE ID : CVE-2019-9050		
N/A	23-02-2019  5.8  Pluck 4.7.9-dev1. The CSRF vulnerability delete articles via a		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)	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=deleteimag e&var1= URI.  CVE ID: CVE-2019-9052	N/A	A-PLU-PLUC- 030419/225
podofo_proje	ect				
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://b ugzilla.re dhat.com /show_bu g.cgi?id=C VE-2019- 3812	A-QEM- QEMU- 030419/227

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID						atch	NCII	PC ID
			CVE ID : CVE-2019-3812								
responsive_v	rideo_news_sci	ript_pr	oject								
responsive_v	rideo_news_sci	ript									
N/A	16-02-2019	4.3	Video the So exam inject	earch Ba	cript ha ir. This r everaged RL redii	s XSS via night, for d for HT rection.	r	N/A			-RESP- 9/228
schoolcms											
schoolcms											
N/A	26-02-2019	6.5	file up featur admin =save exten Conte and p JPEG allow PHP o	pload via re at n.php?m e by usin sion, cha ent-Type dacing P data. Th	a the log =admin g the .jp anging t to imag HP code is ultimation of an	he ge/php, after th ately rbitrary	d &a e	N/A		A-SCH 03041	-SCHO- 9/229
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&a ction=add URI, a related issue to CVE-2018-19332.  CVE ID: CVE-2019-9040					N/A		A-S-C- 03041	
seacms											
seacms											
CV Scoring Sca (CVSS)	le 0-1 ype(s): CSRF- Cross	1-2	2-3	3-4	4-5	5-6	6-7 versal:		7-8	8-9	9-10 n: DoS-
vaniciability I	Denial of Service					-	-				, 503-

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.	N/A	A-SEA-SEAC- 030419/231
seafile			CVE ID : CVE-2019-8418		
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_cr	ns				
N/A	23-02-2019	6.5	An issue was discovered in Sitemagic CMS v4.4. In the index.php?SMExt=SMFiles UF the user can upload a .php file execute arbitrary code, as demonstrated by 404.php.  CVE ID: CVE-2019-9042	•	A-SIT-SITE- 030419/233
Solarwinds					
orion_netwo	ork_performan	ce_mor	nitor		
N/A	18-02-2019	10	SolarWinds Orion NPM befor 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 Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
(CVSS)	CORE CHOSE	Sito Pog	uest Forgery; Dir. Trav Directory Trav	versal: +Info- Gain	Information: DoS

Vulnerability Type(s)	Publish Date	cvss	·						Patch	NCII	PC 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 I	D : CVE	-2019-8	917					
Splunk											
Splunk											
N/A	20-02-2019	3.5	Enter 6.4.x l 6.3.12 before 6.0.15 6.6.0	prise 6 before 6 2, 6.2.x b e 6.1.14 5 and Sp	efore 6. and 6.0	e 6.5.5, x before 2.14, 6.1 x before ht befor	e.x	N/A	A		-SPLU- 9/235
			CVE I	D : CVE	-2019-5	727					
Sqlalchemy											
Sqlalchemy											
N/A	19-02-2019	7.5	1.3.x t SQL II paran	through njection neter.	1.3.0b2	order_by		N/A	A	_	-SQLA- .9/236
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		-ELFI- .9/237	
sublimetext											
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-1		7-8	8-9	9-10
Vulnerability T	ype(s): CSRF- Cross Denial of Service	_	_			_					n; DoS-

Vulnerability Type(s)	Publish Dat	e CVSS	De	escription & C\	/E ID	P	atch	NCII	PC ID
sublime_text	_3	<u> </u>	<u> </u>						
N/A	25-02-2019	9 6.8	possible version 3 bit Wind a Trojan fibers-l1-core-loca may be less blime_file within %LOCAL blime_test vendor's not appe Sublime with Wir patched.	TED ** DLL hin Sublime T 3.1.1 build 31 ows platform horse api-ms -1-1.dll or apalization-l1-2 baded if a victext.exe to open an attacker APPDATA% oxt folder. NO position is "ar to be a bug Text, but rathed ows that had ows that had ows that had the content of	ext 3 76 on 32- as because s-win-core i-ms-win1.dll file tim uses pen a .txt 's 'Temp\su ΓE: the Γhis does g with her one as been		A		-SUBL- 9/238
tautulli								•	
tautulli									
N/A	19-02-2019	4.3	html in T via a craf is mishar construc	erfaces/defau 'autulli 2.1.26 fted Plex user adled when ting the Histo CVE-2019-8	has XSS rname that ory page.		Α	A-TAU TAUT- 03041	
themerig									
find_a_place_	cms_directo	ory							
N/A	16-02-2019	7.5	Themerig Find a Place CMS Directory 1.5 has SQL Injection via the find/assets/external/data_2.ph p cate parameter.  CVE ID: CVE-2019-8360			N/A	A		E-FIND- 9/240
CV Scoring Sca (CVSS)	0-1	1-2		3-4 4-5 ; Dir. Trav Dire	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
tintin_projec	t				
tintin					
N/A	the strip_vt102_codes function in TinTin++ 2.01.6 and WinTin++ 2.01.6 allows remote attackers to execute arbitrary		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.	N/A	A-TIN-TINT- 030419/241
wintin			CVEID: CVE 2017 7027		
WIIIUII	I			1	
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_pi	roiect				
tiny_issue	<u> </u>				
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/configsetup.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			0.212.0.2 2017 7002		
TOR					
TUK					

CV Scoring Scale (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-

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCII	PC ID
N/A	21-02-2019	5	befor 0.3.5. alpha again can o exhau sched	e 0.3.4.1 8, and 0 , remote st Tor cl ccur via ustion in	1, 0.3.5. 4.x befo denial	T cell	.2- :e	N/	A	A-TOR 03041	
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	index as der a=ind	.php?c= monstra lex[XSS]	main a p ted by a			N/.	A	A-VER VERY- 03041	
vnote_projec	t										
vnote											
N/A	17-02-2019	4.3	note.	VNote 2.2 has XSS via a new text note.  CVE ID: CVE-2019-8419				N/	A	A-VNC VNOT- 03041	
wavemaker											
wavemarker	_studio										
N/A	21-02-2019	6.8	com/wavemaker/studio/Studio Service.java in WaveMaker Studio 6.6 mishandles the studioService.download?metho					A	A-WAV- WAVE- 030419/248		
CV Scoring Scal	le 0-1	1-2	<b>2-3 3-4 4-5 5-6 6-7 7-8 8-9</b>						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/WebKitWeb ViewGtk.cpp, as demonstrated by GNOME Web (aka Epiphany).	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

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/WebKitScri ptDialogGtk.cpp, UIProcess/API/gtk/WebKitScri ptDialogImpl.cpp, and UIProcess/API/gtk/WebKitWeb ViewGtk.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.	N/A	A-WIR- WIRE- 030419/251
			CVE ID : CVE-2019-9208		
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

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			dereference of a NULL conversation.  CVE ID: CVE-2019-9214		
Woocomme	rce		0/2/2/0/2 2017 /211		
Woocomme					
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-W00- W00C- 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

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_proje	ct				
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	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
wuzhicms											
wuzhi_cms											
N/A	24-02-2019	4.3	via index.p agecute corefra agecut.	ohp?m: &v=ini ime/ap php.	=attachn t&imgui	CMS 4.1.0 nent&f=i rl=[XSS] f hment/i	m to	N/A	A	A-WU WUZH 03041	
N/A	24-02-2019	4.3	via index.p age&v= corefra ge.php	ohp?m: =add&i ime/ar	=messag usernam	cMS 4.1.0 ge&f=mes le=[XSS] age/mes	ss to	N/A	I	A-WU WUZH 03041	
N/A	24-02-2019	4.3	via index.p o&v=lis to corefra o.php.	ohp?m: sting& ime/ap	=content	CMS 4.1.0  t&f=post  ne=[XSS]  ent/post	inf 	N/A	A	A-WU WUZH 03041	
wuzhicms											
N/A	24-02-2019	4.3	via index.p aiduma corefra	ohp?m: ap&x=  ame/ap	=core&f= [XSS]&y:	CMS 4.1.0 =map&v= =[XSS] to /map.phj	=b	N/A	A	A-WU WUZF 03041	
Zoneminder											
Zoneminder											
N/A	17-02-2019	7.5	ZoneM	inder t	hrough	1.32.3 ha	as	N/A	A	A-ZON	<b>J</b> -
CV Scoring Sca (CVSS) Vulnerability T	ype(s): CSRF- Cross Denial of Servic	_	_	_		=	ersa			8-9 nformatio	9-10 on; DoS-

17-02-2019 17-02-2019	7.5	SQL Injection via the skins/classic/views/events.php filter[Query][terms][0][cnj] parameter.  CVE ID: CVE-2019-8423  ZoneMinder before 1.32.3 has SQL Injection via the ajax/status.php sort parameter.  CVE ID: CVE-2019-8424  includes/database.php in ZoneMinder before 1.32.3 has XSS in the construction of SQL-ERR messages.  CVE ID: CVE-2019-8425  skins/classic/views/controlcap. php in ZoneMinder before 1.32.3 has XSS via the newControl array, as	N/A N/A	ZONE- 030419/265 A-ZON- ZONE- 030419/266 A-ZON- ZONE- 030419/267
17-02-2019		ZoneMinder before 1.32.3 has SQL Injection via the ajax/status.php sort parameter.  CVE ID: CVE-2019-8424  includes/database.php in ZoneMinder before 1.32.3 has XSS in the construction of SQL-ERR messages.  CVE ID: CVE-2019-8425  skins/classic/views/controlcap. php in ZoneMinder before 1.32.3 has XSS via the		ZONE- 030419/266 A-ZON- ZONE- 030419/267
17-02-2019		SQL Injection via the ajax/status.php sort parameter.  CVE ID: CVE-2019-8424  includes/database.php in ZoneMinder before 1.32.3 has XSS in the construction of SQL-ERR messages.  CVE ID: CVE-2019-8425  skins/classic/views/controlcap. php in ZoneMinder before 1.32.3 has XSS via the		ZONE- 030419/266 A-ZON- ZONE- 030419/267
	4.3	ZoneMinder before 1.32.3 has XSS in the construction of SQL- ERR messages.  CVE ID: CVE-2019-8425  skins/classic/views/controlcap. php in ZoneMinder before 1.32.3 has XSS via the	N/A	ZONE- 030419/267
15.00.0040		skins/classic/views/controlcap. php in ZoneMinder before 1.32.3 has XSS via the		A-ZON-
45.00.0040		php in ZoneMinder before 1.32.3 has XSS via the		A-ZON-
17-02-2019	4.3	demonstrated by the newControl[MinTiltRange] parameter.  CVE ID: CVE-2019-8426	N/A	ZONE- 030419/268
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
17-02-2019	7.5	ZoneMinder before 1.32.3 has SQL Injection via the skins/classic/views/control.ph p groupSql parameter, as demonstrated by a newGroup[MonitorIds][] value.  CVE ID: CVE-2019-8428	N/A	A-ZON- ZONE- 030419/270
			CVE ID: CVE-2019-8426  daemonControl in includes/functions.php in ZoneMinder before 1.32.3 allows command injection via shell metacharacters.  CVE ID: CVE-2019-8427  ZoneMinder before 1.32.3 has SQL Injection via the skins/classic/views/control.ph p groupSql parameter, as demonstrated by a newGroup[MonitorIds][] value.  CVE ID: CVE-2019-8428	CVE ID: CVE-2019-8426  daemonControl in includes/functions.php in ZoneMinder before 1.32.3 allows command injection via shell metacharacters.  CVE ID: CVE-2019-8427  ZoneMinder before 1.32.3 has SQL Injection via the skins/classic/views/control.ph p groupSql parameter, as demonstrated by a newGroup[MonitorIds][] value.

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.	N/A	A-ZON- ZONE- 030419/271
			CVE ID : CVE-2019-8429		
zzcms					
zzcms				T	
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.	N/A	A-ZZC-ZZCM- 030419/272
			CVE ID : CVE-2019-8411		
N/A	as sCrIpT.		arbitrary user/ask.php?do=modify parameter because inc/stopsqlin.php does not block a mixed-case string such as sCrIpT.	N/A	A-ZZC-ZZCM- 030419/273
			CVE ID : CVE-2019-9078		
zzzcms					
zzzphp					
N/A	23-02-2019	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	CV Scoring Scale	6-7 7-8	8-9 9-10

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/i nvokefunction&function=call_us er_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=editfi le 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	K				
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://w ww.opens sl.org/ne ws/secad v/201902 26.txt	O-CAN- UBUN- 030419/277

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_ele ment.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

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/regco mp.c, ext/mbstring/oniguruma/regex ec.c, ext/mbstring/oniguruma/regpa	N/A	O-CAN- UBUN- 030419/281

Vulnerability Type(s)	Publish	Date	cvss		Descrip	otion & C\	/E ID		P	atch	NCI	IPC ID
				unico ext/m tf32_l regula conta seque	de.c, and bstring be.c when ar expresing invalues.	d	ittern ibyte					
N/A	22-02-	2019	5	before 7.2.x left before can all serve memorareas in ext/x	e 5.6.40 before 7 e 7.3.1.2 llow a har to cause ory outs in base mlrpc/l	, 7.x befo .2.14, ar xmlrpc_o ostile XN se PHP t ide of al 64_deco	decode() ALRPC o read located de_xmlr	6,	N/A	1	0-CAN UBUN 03041	
N/A	26-02-	2019	6.8	exists Image at Str that c trigge PDF f binary cause (Segn have	estream eam.cc i an (for e ered by s ile to the y. It allo Denial nentatio unspeci	example example sending e pdfimates an at of Service of fault)	a crafted ages tacker to ce or possiler impac	ed ) il o bly	N/A	1	O-CAN UBUN 03041	
Cisco												
N/A	28-02-	2019	10			ty in the interfac	web-base of the	sed	N/A	1		-RV11- 19/284
CV Scoring Sca (CVSS) Vulnerability Ty	·	)-1 RF- Cross	1-2 Site Req		3-4 gery; Dir.	4-5 Trav Dire	5-6 ectory Trav		; +Inf		8-9	9-10 on; DoS-

Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W Wireless-N PN 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 HTP 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   TV130w_firmware  A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663   TV130w_firmware  A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663   TV130w_firmware  A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663   TV130w_firmware  A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Router versions prior to 1.3.1.1 are affected. CVE ID : CVE-2019-1663	Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCII	IPC ID
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  CV Scoring Scale  0.1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10				Firew Wirel Route Wirel allow remorabite to import to import to import to explorate the affect will wirel wersic affect VPN I 1.3.1.	vall, Cisc ess-N Mer, and Cess-N Varian unaute attacker ary code. The varied data gement actions HT ted devicted decute arlying operations prious HT functions prious RV1 functions prious prio	o RV130 ultifunc isco RV2 PN Rout ithentica er to ex e on an a ulnerabi validatio in the w interfac d exploit by sendi TP reque ce. A suc allow th oitrary c perating evice as r. RV110 PN Firev r to 1.2.2 30W Wi a VPN Ro r to 1.0.3 15W Wi ersions fected.	tion VPN 215W er could ated, ecute affected lity is du n of user veb-base e. An t this ing ests to a ccessful e attacke ode on the system of a high- W vall 2.1 are reless-N outer 3.45 are reless-N prior to	leer he				
M/A  28-02-2019  10  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  CV Scoring Scale  0.1  1-2  2-3  3-4  4-5  5-6  6-7  7-8  8-9  9-10	rv130w_firm	ware										
- II-I I I-X I X-4 I X-5 I 5-6 I 6-7 I X-9 I X-9 I Y-ΙΙΙ	N/A	28-02-2019	10	management interface of the Cisco RV110W Wireless-N VPN Firewall, Cisco RV130W Wireless-N Multifunction VPN Router, and Cisco RV215W  O-CIS-RV1 030419/2								
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.	(CVSS)	ype(s): CSRF- Cross	-				=	ersal	; +Inf		8-9 nformatio	9-10 on; DoS-

			remote arbitre device to implement attack vulne malice target explo	te attack rary code. The vi- proper vi- ied data gement ker could rability ious HT' ted devi-	validation in the w interface d exploit by sendi	ecute affected lity is due n of user- veb-based e. An this ng				
			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  A vulnerability in the web-based management interface of the							
rv215w_firmwa	are									
N/A 28	8-02-2019	10	mana Cisco Firew Wirel Route Wirel allow remote arbitr device	gement RV110V vall, Cisc ess-N M er, and C ess-N VI an unau te attack cary code	interface W Wirele o RV130 fultifunct lisco RV2 PN Route uthentica ker to exe e on an a	e of the ess-N VPN W tion VPN 215W er could ated, ecute	N/A	A	0-CIS- 03041	RV21- 9/286
CV Scoring Scale (CVSS) Vulnerability Type(		1-2 Site Regi	2-3	3-4 gery: Dir.	4-5	5-6	6-7	7-8 fo- Gain Ir	8-9	9-10

Vulnerability Type(s)	Publ	lish Date	cvss		Descrip	tion & C\	/E ID		F	Patch	NCI	IPC ID
				mana attack vulne malic targe explo to execunder the af privil Wirel version affect Multi version affect VPN I 1.3.1.	gement ker could rability ious HT ted devi it could ecute arlying opfected dege user ess-N V ons prious pri	interfaced exploited by sends TP requece. A success allow the pitrary of the contrary of the c	t this ing ests to a ccessful e attacke ode on the system of a high- W vall 2.1 are reless-N outer 3.45 are reless-N prior to	er ne				
hyperflex_hx	_data	_platfor	m									
N/A	21-0	2-2019	service Softwom unaut to gai in the is due attack wilnes the him privile succes the atto all	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					A		-HYPE- 19/287	
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8	8-9	9-10
Vulnerability T			-				ectory Trav njection; N					on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Type(s)	21-02-2019	4.3	HyperFlex Software Releases prior to 3.5(2a).  CVE ID: CVE-2019-1664  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.	N/A	O-CIS-HYPE- 030419/288
N/A	21-02-2019	5	Versions prior to 3.5(1a) are affected.  CVE ID: CVE-2019-1665  A vulnerability in the Graphite service of Cisco HyperFlex software could allow an unauthenticated, remote attacker to retrieve data from the Graphite service. The	N/A	O-CIS-HYPE- 030419/289

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCII	PC ID
				explosendi Grapi explo to ret the G	rols. An a bit this voing craft hite serve bit could trieve an raphite to 3.5(2	ulnerabi ed reque ice. A su allow th y statist service. a) are a	lity by ests to th ccessful e attack ics from Versions fected.	l er				
N/A	21-	02-2019	2.1	interior softwall author write Graph vulne insufficient contraction allow arbits which statis interior 3.5(2)	nerability face of Corare could renticated arbitrate interability ficient arbitris vole. An arbit this vole and so are afface. Veral) are afface. Veral) are afface.	d allow l, local a ry data t rface. Th is due to uthoriza ttacker ulnerabi the Gra ending a ssful exp cker to a to Grap result in ag presens sions pr fected.	perFlex an ttacker to the tion could lity by phite rbitrary loit coul write ohite, invalid nted in to	, ld	N/	A	0-CIS- 03041	
ios_xr												
N/A	21-	02-2019	5	servi Conv Serie unau attac	nerabilit ce of Cis ergence s softwa thentica ker to re	co Netw System re could ted, rem trieve a	ork 1000 allow a ote bitrary		N/	A	0-CIS- 03041	_
CV Scoring Sca (CVSS)	le	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.

			possibly result information of vulnerability validation of input within processed by software. An exploit this vulnerability validation of input within processed by software. An exploit this vulning director techniques in requests sent service on a texploit could to retrieve and the targeted of the disclosure information.	disclosure.  is due to in user-suppl TFTP requ the affecte attacker co ulnerabilit bry traversa malicious t to the TFT cargeted de allow the bitrary file device, resi	mproper lied ests ed ould y by al FP evice. An attacker es from ulting in				
			affects Cisco I releases prior for Cisco Nets System 1000 when the TFT enabled.  CVE ID : CVE	IOS XR Sof r to Releas work Conv Series dev TP service	rability tware te 6.5.2 rergence rices is				
spa112_firmware									
N/A 25-02	2-2019 5	5.8	A vulnerability handling come Cisco SPA112 SPA5X5 Series allow an unautemote attack control some Transport Le encrypted Series Protocol (SIP vulnerability improper val certificates. A	nponent of 2, SPA525, es IP Phone uthenticate ker to liste aspects of evel Securities on Initial 2) conversatis due to the didation of state of the security o	the and es could ed, n to or factor ation the server	N/A	A	0-CIS-: 03041	
CV Scoring Scale (CVSS)	0-1 1-2	2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Type(s): C		_	est Forgery; Dir.		-			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	P	Patch	NCII	PC ID
			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 SPA5112 Series IP Phones.	У			
spa500_firm	ware						
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	- N/A	A	0-CIS- 03041	
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7	7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directory Traver oss Site Scripting; Sql- SQL Injection; N/A 97			nformatio	n; DoS-

Vulnerability Type(s)	Publis	h Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
				by an softw of the SPA5 Cisco Series Cisco Series Cisco Series	affected are included Cisco S 25 Serie Small B is IP Pho of the Ci Small B is IP Pho	rect calls I device. Ude vers I Pho Usiness I Sco Sma	Affected ion 7.6.2 siness and SPA5X5 version all Busin nes and SPA112	d 2 ess				
spa500ds_fir	mware											
N/A	25-02-	-2019	5.8	handle Cisco SPA5: allow remo contre Transencry Proto vulne improcertificant attack encry route by an softwoof the SPA5	ing com SPA112 X5 Serie an unaute attack of some sport Le pted Serie col (SIP rability oper val icates. A it this val icate to a a ma icate to a redir affected are included	cy in the ponent of ponent	of the 5, and nes could ated, ten to of a rity (TLS tiation sation. To the of server to the d allow potentials initiate Affected ion 7.6.2 siness nes and	ld r S)- The an ally d d 2	N/A			-SPA5- 19/294
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10
Vulnerability T			_			Trav Dire Sql- SQL Ir	-					on; DoS-

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.		
spa500s_firm			CVE ID : CVE-2019-1683		
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	N/A	O-CIS-SPA5- 030419/295
			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 SPA5112 Series IP Phones.		030417/273

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

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C	VE ID		P	atch	NCI	IPC ID
			CVE I	D : CVE	-2019-1	1683					
spa501g_firm	ıware										
N/A spa502g_firm	25-02-2019	5.8	handle Cisco SPA5 allow remo contre Transencry Protocular improcessing explocation certificattack encry routed by an softwoof the SPA5 Cisco Series 1.4.2 SPA5 Cisco Series contressing explosion of the SPA5 cisco Series for the	span an unaute attack of some sport Le pred Second (SIP p	ponent , SPA52 s IP Pho athentic ser to lis aspects vel Secu ssion Ini ) conver is due to idation o n attack alnerabi licious s present loit coul vesdrop ffic and rect calls I device ude vers mall Bus s IP Pho usiness nes and s IP Pho usiness nes and usiness nes.	5, and ones could ated, sten to or a rity (TLS itiation reation. To the of server to the ld allow potentials initiate and SPA5X5 version all Busines and SPA112	ld r S)- The an an ally d d 2	N/A	<b>A</b>		-SPA5- 19/296
N/A	25-02-2019	5.8	hand	nerabiliting com	ponent		ate	N/A	1		-SPA5- 19/297
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
vuinerability Ty	pe(s): CSRF- Cross Denial of Service	_			Sql- SQL lı	-					on; DoS-

Vulnerability Type(s)	Publi	sh Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
				allow remote contractions and software of the SPA5. Cisco Series 1.4.2 SPA5. Cisco Series of the ser	an unaute attack of some sport Legard Services. A service to early affected are included affected affect	athenticater to list aspects wel Secures on Initial (Secures of Secures of Se	ten to or of a rity (TLS tiation sation. To the of server ter could lity by erver to the d allow a on TLS-potentia sinitiated from 7.6.2 siness nes and SPA5X5 version all Busines and SPA112	he an lly				
spa504g_firm	ware											
N/A	25-02	2-2019	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				d	N/A	A		-SPA5- 19/298
CV Scoring Scal (CVSS) Vulnerability Ty		0-1	1-2	2-3	3-4	4-5	5-6		-7	7-8	8-9	9-10
vuiller ability Ty			_				ictory rrav njection; N					ni, Dus-

Vulnerability Type(s)	Publish Date	cvss		Descrip	otion & C\	/E ID		P	atch	NCI	IPC ID
			vulne impro certification craftical certification attacked encry route by an softwoof the SPA5. Cisco Series 1.4.2 SPA5. Cisco Series S	rability oper val icates. A it this v ng a ma icate to . An exp ker to ea or redin affected are incl care incl care incl solution of the C Small B solution of the C Small B solution of the C Small B solution of the C	) convertis due to idation of an attack ulnerabilicious supresent oloit could rect calls device. The properties and its IP Photosiness and IP Ph	o the of server er could lity by erver to the d allow on TLS potentia initiate Affected ion 7.6.2 siness nes and SPA5X5 version ll Busin nes and SPA112	an - ally d d 2				
spa508g_firm	1ware 25-02-2019	5.8	handle Cisco SPA5: allow remo contraction and the contraction and the contraction are contraction and the contraction are contraction and the contraction are contraction are contraction and the contraction are contraction are contraction and the contraction are contraction and the contraction are contraction and the contraction are cont	ing com SPA112 X5 Serie an unar te attacl ol some sport Le pted Se col (SIP rability oper val icates. A	ty in the aponent 2, SPA52 es IP Pho uthenticater to lis aspects vel Secu idation can attack ulnerabilicious s	of the 5, and nes coul ated, ten to or of a rity (TLS tiation sation. To the of server er could lity by	ld r S)- The	N/A	4		-SPA5- 19/299
CV Scoring Sca (CVSS) Vulnerability Ty	/pe(s): CSRF- Cro	-				-		; +Inf			9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE	ID	Patch	NCIII	PC ID
			certificate to present to client. An exploit could a attacker to eavesdrop or encrypted traffic and por route or redirect calls in by an affected device. Af software include version of the Cisco Small Busin SPA525 Series IP Phone Cisco Small Business SP. Series IP Phones and version of the Cisco Small Business SP. Series IP Phones and version of the Cisco Small Business SP. Series IP Phones and Version SPA500 Series IP Phone Cisco Small Business SP. Series IP Phones.	allow an n TLS- otentially nitiated ffected in 7.6.2 less and A5X5 rsion Business and A112			
spa509g_firm	 nware		0.2.15.10.2.2017.100				
N/A	25-02-2019	5.8	A vulnerability in the ce handling component of Cisco SPA112, SPA525, a SPA5X5 Series IP Phone allow an unauthenticate remote attacker to lister control some aspects of Transport Level Security encrypted Session Initia Protocol (SIP) conversation vulnerability is due to the improper validation of secretificates. An attacker exploit this vulnerability crafting a malicious servicertificate to present to client. An exploit could a attacker to eavesdrop or encrypted traffic and por route or redirect calls in by an affected device. Af	the and es could ed, n to or a y (TLS)-ation tion. The he server could y by ver the allow an n TLS-otentially nitiated	N/A	0-CIS- 03041	
CV Scoring Sca (CVSS)	0-1	1-2	<b>2-3</b> 3-4 4-5	5-6 6-7	7 7-8	8-9	9-10
		_	uest Forgery; Dir. Trav Directo oss Site Scripting; Sql- SQL Injec 103			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		Patch	NCI	IPC ID
			of the SPA5 Cisco Series 1.4.2 SPA5 Cisco Series	e Cisco S 25 Serie Small B s IP Pho of the Ci 00 Serie Small B s IP Pho	mall Bus IP Pho usiness Sines and sines Sma IP Pho usiness Siness	nes and SPA5X5 version Ill Busine nes and SPA112				
spa512g_firn	ıware		OVE.	D T G T E						
N/A	25-02-2019	5.8	handle Cisco SPA5 allow remo contre Trans encry Proto vulne improcertification craftic certificattack encry route by an softwoof the SPA5 Cisco Series	spannant spa	ponent of ponent of ponent of ponent of ponent of ponent of the ponent o	5, and nes coulated, ten to or a rity (TLS tiation sation. To the of server to the d allow a potential initiated Affected ion 7.6.2 siness nes and SPA5X5	d . f)- The N an Illy d I	/A		-SPA5- 19/301
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		Patch	NCI	IPC ID
			Cisco		s IP Pho usiness : nes.					
			CVE I	D : CVE	2019-1	683				
spa514g_firn	nware		1						<u> </u>	
N/A	25-02-2019	5.8	handle Cisco SPA5 allow remo contre Trans encry Proto vulne improcertificattack encry route by an softw of the SPA5 Cisco Series 1.4.2 SPA5 Cisco Series	spannant te attack of some sport Legardility oper validicates. An expect to early or redinaffected are included affected affected affected affected are included affected	y in the ponent of ponent	of the 5, and nes could ated, ten to or a rity (TLS tiation sation. To the of server to the d allow on TLS potentials initiate Affected ion 7.6.2 siness nes and SPA5X5 version all Busines and SPA112	an an allly d	/A		-SPA5- 19/302
spa525_firm	ware									
CV Scoring Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		Р	atch	NCI	IPC ID
N/A	25-02-2019	5.8	hand Cisco SPA5 allow remo contr Trans encry Proto vulne impro certif explo crafti certif client attack encry route by an softw of the SPA5 Cisco Series	spannante attack an unaute attack of some sport Lerpted Services (SIP brability oper valuicates. An expect to ear or redinaffected are included affected are included affected spannante s	ponent of SPA52 is IP Phoenthenticater to list aspects well Securistion Initial (Conversion attack alnerabilicious supresent loit coull vesdrop ffic and rect calls ledevice. The lade version attack alnerabilicious supresent loit coull vesdrop ffic and rect calls ledevice. The lade version and ledevices and susiness and second sec	5, and nes coulated, ten to or of a rity (TLS tiation sation. To the of server to the dallow a non TLS-potential initiated ion 7.6.2 siness nes and SPA5X5 version all Busines and SPA112	d ())- ()he	N/A	<b>A</b>		-SPA5- 19/303
spa525g_firm	ıware										
N/A	25-02-2019	5.8	hand Cisco SPA5 allow	ling com SPA112 X5 Serie an unau	ponent of SPA52 s IP Pho	5, and nes coul	d	N/A	<b>A</b>		-SPA5- 19/304
CV Scoring Sca (CVSS)	le <b>0-1</b>	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID		Patch	NCII	PC 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_firm	ware						
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 Sca (CVSS)	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7	7 7-8	8-9	9-10
	unals): CSPE_Cross	Sito Pog	uest Forgery; Dir. Trav Directory	Traversalı	+Info Gain I	nformatio	n: DoS-

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID		Patch	NCII	PC ID
			certificates. An attaexploit this vulneral crafting a malicious certificate to present client. An exploit contact attacker to eaves directly an affected devisoftware include very of the Cisco Small Busines Series IP Phones at 1.4.2 of the Cisco Small Busines SPA500 Series IP Phones.  CVE ID: CVE-2019	ability by a server at to the buld allow a cop on TLS and potentialls initiated ersion 7.6.2 Business thones and as SPA5X5 and version mall Busine thones and as SPA112	an - ally d 1			
firepower_90	000_firmware			1005				
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		e N, on ice as.	/A	O-CIS-FIRE- 030419/306	
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability T		_	uest Forgery; Dir. Trav I oss Site Scripting; Sql- SQ 108	<del>-</del>			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Citrix			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.  CVE ID: CVE-2019-1700		
	plication_deliv	ery_co	ntroller_firmware		
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- 030419/307
netscaler_ga	teway_firmwa	re			

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Type(s): CSRE- Cross Site Request Forgery: Dir. Tray - Directory Trayersal: +Info- Gain Information: DoS-											

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 69.5 and Application Delivery Controlle (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 a TLS Padding Oracle Vulnerability when CBC-based cipher suites are enabled.	of	O-CIT-NETS- 030419/308
dasannetwor	rks				
h665_firmwa	ire				
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 admaccount via TELNET.  CVE ID: CVE-2019-8950	/	O-DAS- H665- 030419/309
D 11			CVE ID : CVE-2019-0950		
Debian					
debian_linux			xc 1, .		
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, as once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record in	ws/secad v/201902 26.txt	O-DEB-DEBI- 030419/310
CV Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
		received with invalid compared to if a 0 by received with an invathe application then differently based on way that is detectable remote peer, then the to a padding oracle the used to decrypt da order for this to be exponentially a compared to the use. Stitch ciphersuites are optimized implementations of a commonly used ciphersuites are optimized to the application of the common of the compared to the protocol error has obtained but some do anyway openSSL 1.0.2r (Affer 1.0.2q).			
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)	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.	N/A	O-DEB-DEBI- 030419/313
			CVE ID: CVE-2019-5756		
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-

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.	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

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.	N/A	O-DEB-DEBI- 030419/322
			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.	N/A	O-DEB-DEBI- 030419/323
			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.	N/A	O-DEB-DEBI- 030419/324
			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	N/A	O-DEB-DEBI- 030419/325

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.	N/A	O-DEB-DEBI- 030419/326
			CVE ID : CVE-2019-5770		
N/A	19-02-2019	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	O-DEB-DEBI- 030419/327
			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.	N/A	O-DEB-DEBI- 030419/328
			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-DEB-DEBI- 030419/329

Vulnerability Type(s)	Pul	blish Date	cvss		Descrip	otion & C\	/E ID		ı	Patch	NCII	PC ID
N/A	19-	02-2019	4.3	confu Omni prior remo conte bar)	isable chailbox in Good to 72.0. te attackents of the via a cra	idling of naracter loogle Cl 3626.81 ker to sp ne Omnil fted don	in nrome allowed oof the oox (UR) nain nan	L	N/	A	O-DEB 03041	-DEBI- 9/330
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.						A	O-DEB 03041	-DEBI- 9/331
N/A	19-	02-2019	4.3	Incor confu Omni prior remo conte bar)	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.					A	O-DEB 03041	-DEBI- 9/332
N/A	19-	02-2019	4.3	A mis speci reque Goog 72.0 attack to ins to by check crafte	CVE ID: CVE-2019-5777  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					A	O-DEB 03041	-DEBI- 9/333
N/A	19-	02-2019	4.3	Insuf	Insufficient policy validation in					A	O-DEB	-DEBI-
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

(CVSS) 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		Descrip	tion & C	/E ID		P	atch	NCII	PC ID
			Chron allowe bypas via a c	ne prioned a ren s naviga rafted l	er in Goo to 72.0 note atta ation res	.3626.81 acker to striction age.				03041	9/334
					-2019-5						
N/A	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 JayaScript via Apple Events.		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.						O-DEB 03041	-DEBI- 9/335	
			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.						A	O-DEB 03041	-DEBI- 9/336
					-2019-5						
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						Α	O-DEB 03041	-DEBI- 9/337
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.						A	O-DEB 03041	3-DEBI- 9/338
CV Scoring Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	F	Patch	NCII	PC ID		
			access or rea relate in ext/x ment.	s (heap ad after : ad to xm mlrpc/l: c.	alid menout of booking of the office of the						
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.					N/A	A	O-DEE 03041	3-DEBI- 9/343
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						A	O-DEE 03041	s-DEBI- 9/344
CV Scoring Sca (CVSS)	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
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/regco mp.c, ext/mbstring/oniguruma/regex ec.c, ext/mbstring/oniguruma/regpa 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	O-DEB-DEBI- 030419/345
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-DEB-DEBI- 030419/346
N/A	26-02-2019	6.8	A heap-based buffer underwrite exists in	N/A	O-DEB-DEBI- 030419/347

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & C\	/E ID		Р	atch	NCII	PC ID
			ImageStream at Stream.cc that can (for triggered by PDF file to the binary. It allocause Denial (Segmentation have unspective CVE ID : CVE	in Popple example sending le pdfimatows an ato of Service of fault)	er 0.74.0 ) be a crafted ages tacker to ce or possile	l o oly				
N/A	27-02-2019	4.3	In AdvanceC png_compre advpng has a upon encour PNG size, whattempted material abuffer that is also a hear read.)  CVE ID: CVE	ss in png in intege: itering ar ich resul emcpy to is too sm o-based b	ex.cc in roverflo invalid ts in an owrite in all. (The	nto	N/A	A	_	3-DEBI- 9/348
Dlink										
dir-823g_firn	nware									
N/A	16-02-2019	5	An issue was Link DIR-82: firmware 1.0 incorrect acc allowing ren enable Guest SetWLanRac API to the wa by /bin/goal	3G device 2B03. The ess control of attack wi-Fi vinosetting eb serviced.	es with nere is rol ckers to a the gs HNAP e provide		N/A	Α	0-DLI 03041	-DIR .9/349
D-link										
dir-825_rev.b	_firmware									
N/A	25-02-2019	6.5	An issue was	discove	red on D	-	N/A	Λ	O-D-L	-DIR
CV Scoring Scal (CVSS)	0-1	1-2	2-3 3-4	4-5	5-6	6-		7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service		uest Forgery; Dir. oss Site Scripting;							n; DoS-

table, firmware version, update time, QOS information, LAN information of the device.  CVE ID: CVE-2019-9126  dir-878_firmware  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  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  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  CV Scoring Scale  OLD-L-DIR-030419/354	Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID
N/A 25-02-2019 7.5 Link DIR-825 Rev.B 2.10 devices. The "user" account has a blank password.  CVE ID: CVE-2019-9123  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 of the device.  CVE ID: CVE-2019-9126  dir-878_firmware  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  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  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  CV Scoring Scale  O-D-L-DIR-030419/354					devic attacl comn parar POST	es. They kers to e nands vi neter in request	allow re execute a a the ntp an ntp_s	emote rbitrary o_server sync.cgi				03041	19/350
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 of the device. CVE ID: CVE-2019-9126  dir-878_firmware  An issue was discovered on D- Link DIR-878 1.12B01 devices. At the /HNAP1 URL, an attacker can log in with a blank password. CVE ID: CVE-2019-9124  An issue was discovered on D- Link DIR-878 1.12B01 devices. At the /HNAP1 URL, an attacker can log in with a blank password. CVE ID: CVE-2019-9124  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  CV Scoring Scale  D. 1. 1.2 2.3 3.4 4.5 5.6 6.7 7.8 8.9 9.10	N/A	25-	02-2019	7.5	Link l devic a blar	DIR-825 es. The ' nk passv	Rev.B 2 'user" ac vord.	.10 ecount h		N/A	A		
Mr/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  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  CV Scoring Scale  O-D-L-DIR-030419/353	N/A	25-	02-2019	5	Link link link device disclored documents of the contraction of the co	DIR-825 es. Ther osure vu ests for t ment. Th ode, MA firmwa QOS inf mation,	Rev.B 2 e is an ir lnerabil the route nis will re C addres re version ormation and WLA of the de	.10  nformati ity via er_info.xi eveal the ess, routin on, upda n, LAN AN vice.	on ml e ng	N/A	A		
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  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  CV Scoring Scale  O-D-L-DIR-030419/353  O-D-L-DIR-030419/354	1' 070 C				CVE I	D : CVE	-2019-9	126					
N/A  25-02-2019  7.5  Link DIR-878 1.12B01 devices. At the /HNAP1 URI, an attacker can log in with a blank password.  CVE ID: CVE-2019-9124  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  CV Scoring Scale  O-D-L-DIR-030419/353	dir-878_firm	war	e					1 5		I			
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  CV Scoring Scale  0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	N/A	25-	02-2019	7.5	Link land the can lo	DIR-878 e /HNAF og in wit vord.	1.12B0 21 URI, a h a blan	1 device: n attack k	S.	N/A	A		
-	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				S.	N/A	I		
(CVSS)  Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-	(CVSS)												

Google Android  N/A 28			In SkS SkSwiz possib	NAP_AU  O: CVE  wizzler  zzler.cp	-2019-9 -::onSetS	SampleX c					
Android			In SkS SkSwiz possib	wizzler zzler.cp	r::onSetS	SampleX c	of				
Android			SkSwiz possib	zzler.cp	p, there	-	of				
	0.00.0040		SkSwiz possib	zzler.cp	p, there	-	of				
N/A 29	0.00.0040		SkSwiz possib	zzler.cp	p, there	-	of				
11/11 20	8-02-2019	9.3	This constraints and dition needed Production Andro 11783	ould leation of place on all executed the control of the control o	ad to ren privilege er with n ecution p interact xploitation roid. Ven ndroid II	ls write nds check note e in o privileges ion is on. rsions: D: A-	5	https:, ource. roid.co securi bulleti 2019- 01	and om/ ty/ in/	0-G00 ANDR 03041	
N/A 28	8-02-2019	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:; ource. roid.co securi bulleti 2019- 01	and om/ ty/ in/	0-G00 ANDR 03041	
N/A 28	8-02-2019	9.3	there i	s a pos		zler.cpp, t of bound r input	ds	https: ource. roid.co	and	O-GOO ANDR 03041	
CV Scoring Scale (CVSS) Vulnerability Type(		1-2	2-3	3-4	4-5	5-6	6-7		7-8	8-9	9-10

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://s ource.and roid.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://s ource.and roid.com/ security/ bulletin/ 2019-02- 01	0-G00- ANDR- 030419/359

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		ı	Patch	NCII	PC ID				
				ID: A-	-116222	069.										
				CVE I	D : CVE	-2019-1	992									
N/A	28-	02-2019	7.2	there corru overf local no ad privil intera explo Versi 8.1 A 1198	gister_ap is a pos- iption du low. Thi escalational eges need action is itation. I ons: And ndroid-9	sible me ne to an i s could l on of pri execution eded. Use not need Product: lroid-8.0	mory integer ead to vilege w on er ded for Android O Android id ID: A-	d. d-	oui roi sec bul	ps://s rce.and d.com/ urity/ letin/ 19-02-	O-GOO ANDR 03041					
					D : CVE	-2019-1	993									
N/A	28-	02-2019	9.3	Development of the period due to access with privile interaction of the period of the	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				oui roi sec bul	ps://s rce.and d.com/ rurity/ letin/ 19-02-	0-G00 ANDR 03041					
N/A	28-	02-2019	2.1	Comp there silent due to could	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://s ource.and roid.com/ security/ bulletin/ 2019-02-		0-G00- ANDR- 030419/362					
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6 -		-7	7-8	8-9	9-10				
vuinerability Ty			_			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.										

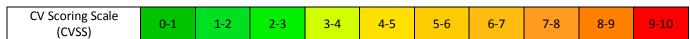
Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			accessible to AOSP Mail to a remote email recipient, with no additional execution privileges needed. User interaction is not needed for exploitation.  Product: Android. Versions: Android-7.0 Android-7.1.1 Android-7.1.2 Android-8.0 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://s ource.and roid.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://s ource.and roid.com/ security/ bulletin/ 2019-02- 01	0-G00- ANDR- 030419/364

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	otion & C\	/E ID		F	atch	NCI	IPC ID
				Andr		Android-	ndroid-8 ·9. Andro					
				CVE I	D : CVE	-2019-1	997					
N/A	28-	02-2019	4.9	keym possi due to reboo denia by a f addit needo Produ Andro	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  In hinder alloc free page of				0-G00 ANDR 03042			
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	A	O-GOO ANDR 03042		
N/A	28-	02-2019	7.2	there corru free. ' escala	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 Sca (CVSS)	le	0-1	1-2	2-3	3-4	4-5	5-6	6-	7	7-8	8-9	9-10

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://s ource.and roid.com/ security/ bulletin/ 2019-02- 01	O-GOO- ANDR- 030419/368
Linux			0VE1D: 0VE 2017 2001		
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	0_1	1_2	2_2	2_/1	4-5	5-6	6-7	7₋0	Q_Q	0-10
(CVSS)	0-1	1-2	2-3	3-4	4-3	3-0	6-7	7-8	8-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	22-02-2019	In the Linux kernel before 4.20.5, attackers can trigger a drivers/char/ipmi/ipmi_msg ndler.c use-after-free and 000 by arranging for certain simultaneous execution of the code, as demonstrated by a "service ipmievd restart" loop CVE ID: CVE-2019-9003 In the Linux kernel before		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_pers	eus-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_db g.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



Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID		P	atch	NCII	PC ID
			device.					
			CVE ID : CVE-2019-9111					
N/A	24-02-2019	7.1	The msm gpu driver for custor 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 count argument in _sde_debugfs_conn_cmd_tx_we in drivers/gpu/drm/msm/sde/e_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	the vrit 'sd	N/A			-XIAO- 9/374
Mikrotik			CVEID. CVE 2017 7112					
Routeros								
N/A	20-02-2019	5	MikroTik RouterOS before 6.43.12 (stable) and 6.42.12 (long-term) is vulnerable to a intermediary vulnerability. T 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	he	N/A		O-MIK ROUT- 03041	-
netis-system								
wf2411_firm							ı	
N/A	21-02-2019	9	On Netis WF2880 and WF242	11	N/A	<b>L</b>	O-NET	`-
CV Scoring Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-		7-8	8-9	9-10
Vulnerability T		_	uest Forgery; Dir. Trav Directory Travoss Site Scripting; Sql- SQL Injection; N 130				ntormatio	n; DoS-

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_firm	ware				
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
Phoenixcont	act				
axc_1050_fir	mware				
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 Sca	le <b>0-1</b>	1-2	<b>2-3 3-4 4-5 5-6 6</b> ·	-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.

(CVSS)

Vulnerability Type(s)	Publish Date	e CVSS		Descrip	tion & C\	/E ID		P	atch	NCI	IPC ID		
			demo Creat	nstrateo e Backu	or make d by usir p featur irectorie	e to	as						
			CVE I	D : CVE	-2019-9	201							
ilc_131_eth/	xc_firmware												
N/A	26-02-2019	9	ILC 13 IL	31 ETH, 51 ETH, LC 191 N, and A remote lish TCP and obt mation constrated Backurse all d	XC, ILC XC, ILC ETH 2T AXC 105 attacke session ain sens or make I by usin p featur irectoric	s to port itive changes, ng the e to es.	I, I 1 s	N/A			D-ILC 19/379		
			CVE I	D : CVE	-2019-9	201							
Phoenix Contact ILC 131 ETH, 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						I, I 1 s	N/A			D-ILC 19/380			
ilc_151_eth/	xc_firmware												
N/A	26-02-2019	9	Phoenix Contact ILC 131 ETH, ILC 131 ETH/XC, ILC 151 ETH, O-PHO-ILC						O-ILC				
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10		
Vulnerability T		-	_	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		Descrip	tion & C\	/E ID		P	atch	NCII	PC 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							03041	9/381
ilc_151_eth_f	irmware										
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	A		)-ILC .9/382	
ilc_171_eth_2	tx_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	Α		)-ILC .9/383
CV Scoring Sca (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-		7-8	8-9	9-10
vallerability I	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; SqI- SQL Injection; N/A- Not Applicable.  133										

				Description & CVE ID					F	atch	INCI	IPC ID		
				trave	rse all d	irectorie	es.							
				CVE I	D : CVE	-2019-9	201							
ilc_191_eth_2	tx_firn	nware												
N/A	26-02	-2019	9	ILC 1: ILC 1: 2TX, I ME/A allow estab 1962 inform demo Creat trave	31 ETH, 51 ETH, ILC 191 AN, and A remote lish TCP and obt mation constrated e Backu rse all d	XC, ILC XC, ILC ETH 2TX AXC 105 attacker session ain sens	s to port itive changes, ag the e to es.	1	N/A			D-ILC 19/384		
ilc_191_me/a	n_firm	ware												
N/A	26-02	-2019	9	ILC 1: ILC 1: 2TX, I ME/A allow estab 1962 inform demo Creat trave	31 ETH, 51 ETH, LC 191 LN, and A remote lish TCP and obt mation constrated e Backu rse all d	XC, ILC XC, ILC ETH 2TX AXC 105 attacked session ain sens	s to port itive changes, ng the e to es.	1	N/A			D-ILC 19/385		
Redhat														
enterprise_li	nux_de	esktop												
N/A	19-02	-2019	4.3	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed				Networking in Google Chrome			N/A		O-REI ENTE 03041	
CV Scoring Scal	le	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7	7-8	8-9	9-10		

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	otion & C\	/E ID			Patch	NCIII	PC ID		
				cause obtain encry	use of a	unning on proxy sext of tra a malicion	server to insport							
				<b>CVE ID : CVE-2019-5754</b>										
N/A	19-	02-2019	5.8	zero i prior remo arbiti crafte	in V8 in to 72.0. te attack ary reaced HTMI		Chrome allowed erform via a		N/A		N/A		O-RED ENTE- 03041	
				CVE I	D : CVE	-2019-5	755							
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.					N/	A	O-RED ENTE- 03041			
				CVE I	D : CVE	-2019-5	756							
N/A	19-	02-2019	6.8	assun Chroi allow poter corru page.	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					A	O-RED ENTE- 03041			
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- 03041			
CV Scoring Sca (CVSS)	le	0-1	1-2	2-3	2-3 3-4 4-5 5-6				-7	7-8	8-9	9-10		

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-

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 Sca (CVSS)	0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

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.		030419/395
			CVE ID: CVE-2019-5763		
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

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-

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		F	atch	NCIII	PC ID
			Googl 72.0.3 attacl heap	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.						ENTE- 03041	
			CVE I	D : CVE	-2019-5	772					
N/A	19-02-2019	4.3	Index prior remo comp proce	tedDB in to 72.0. te attack romisec ss to by	rigin val Google 3626.81 ker who I the ren pass san	Chrome allowed had derer ne origin	l a	N/A	N/A EN 03		
			CVE I	D : CVE	-2019-5	773					
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.				N/A	A	O-RED ENTE- 03041		
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- 03041		
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 Sca	le 0-1	1-2	2-3	3-4	4-5	5-6	6-	-7	7-8	8-9	9-10

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.		
			<b>CVE ID : CVE-2019-5776</b>		
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.	N/A	O-RED- ENTE- 030419/409
			<b>CVE ID : CVE-2019-5777</b>		
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

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.	N/A	O-RED- ENTE- 030419/413
			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	O-RED- ENTE- 030419/414
enterprise_li	niix 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.	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)	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

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	0-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

Vulnerability Type(s)	Pu	blish Date	cvss		Description & CVE ID						NCII	PC ID					
N/A	19-	02-2019	4.3	in the Chron 72.0 attack sensi- proce Inten		er in Goo ndroid p allowed otain pot rmation ory via a	gle rior to a local centially from crafted		N/	A	O-RED ENTE- 03041						
N/A	19-	02-2019	4.3	taint Goog 72.0.: attacl data	ttacker to leak cross-origin ata via a crafted HTML page.  VE ID : CVE-2019-5766  Isufficient protection of					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- 03041							
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				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.		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.		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.		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.		O-RED ENTE- 03041	
N/A	19-	02-2019	6.8	Incorrect handling of invalid					N/	A	O-RED	)-					
CV Scoring Sca (CVSS)	ile	0-1	1-2	2-3	2-3 3-4 4-5 5-6 6			6	-7	7-8	8-9	9-10					

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

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	otion & C\	/E ID		F	Patch	NCII	IPC ID
				policy	via a cı	afted H	ГML pag	ge.				
				CVE II	O : CVE	-2019-5	5773					
N/A	Omission of the filetype from the checklist in Safel Google Chrome of to 72.0.3626.81 attacker who conto download a .d execute arbitrary downloaded .des				the Safe afeBrow ne on Lin 81 allow convinc a .deskto rary cod .desktop	Browsing in nux prioux prioux ded an red a use op file to e via a file.	r	N/A	A	O-REI ENTE 03041		
N/A	19-	-02-2019	4.3	confus Omnik prior t remot conter bar) v	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	O-REI ENTE 03041	
N/A	19-	-02-2019	4.3	confus Omnik prior t remot conter bar) v	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.				N/A	A	O-REI ENTE 03041	
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			Ĺ	N/A	A	O-REI ENTE 03041		
CV Scoring Sca	le	0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10
(CVSS)  Vulnerability T	ype(s)											

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C\	/E ID		F	Patch	NCIII	PC ID
N/A	19-02-2019	4.3	specia reques Google 72.0.3 attack to inst to byp checks	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						0-RED ENTE- 03041	
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	O-RED ENTE- 03041	
N/A	19-02-2019	4.6	can be in Goo prior t local a JavaSc	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.				N/A	A	0-RED ENTE- 03041	
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	A	O-RED- ENTE- 030419/	
N/A	19-02-2019	6.8	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81					N/A		0-RED ENTE- 03041	
CV Scoring Scal	le 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-

Vulnerability Type(s)	Pu	blish Date	cvss		Descrip	tion & C\	/E ID		F	atch	NCII	IPC ID
				execu sandl page.	ed a renate arbitation renate	cary cod crafted	e inside HTML	a				
enterprise_li	nux_	workstat	ion									
N/A	19-	02-2019	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.				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				O-REI ENTE 03041	
N/A	19-	02-2019	5.8	zero i prior remo arbiti crafte	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	Α	O-REI ENTE 03041	
N/A	19-	02-2019	6.8	mana PDFit to 72 remo arbiti via a	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	O-REI ENTE 03041	
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	A	O-REI ENTE 03041	
CV Scoring Sca (CVSS)		0-1	1-2	2-3	3-4	4-5	5-6		-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.  148												

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			page. <b>CVE ID : CVE-2019-5757</b>		
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-

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.		ENTE- 030419/452
			CVE ID : CVE-2019-5762		
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.	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

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 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 Sca (CVSS)	lle 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

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.	N/A	O-RED- ENTE- 030419/461
			CVE ID: CVE-2019-5771  Sharing of objects over calls into		
N/A	19-02-2019	6.8	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 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  Incorrect handling of a confusable character in	N/A	O-RED- ENTE- 030419/464 O-RED- ENTE-
CV Scoring Sco	le le		confusable character in		ENTE-
CV Scoring Sca (CVSS)	0-1	1-2	<b>2-3</b> 3-4 4-5 5-6 6	5-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss		Descrip	tion & C	/E ID		ı	Patch	NCII	PC ID
			remote content	72.0. attack s of th	3626.81 xer to sp ie Omni	allowed	L			03041	9/465
			CVE ID : CVE-2019-5775								
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	O-RED ENTE- 03041	
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	O-RED ENTE- 03041	
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	O-RED- ENTE- 030419/		
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 Sca (CVSS)	le 0-1	1-2	2-3	3-4	4-5	5-6	6	-7	7-8	8-9	9-10

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_li	nux				
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

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