

National Critical Information Infrastructure Protection Centre Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Mar 2019

Vol. 06 No. 05

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCII	PC ID
			Applica	tion					
1024tools									
1024tools									
N/A	12-03-2019	4.3	DOM-based 1024Tools via vectors ' <embed SRC="data: ' substring.</embed 	Markdow involving image/sv	n 1.0 the g+xml	N/A		A-102 04041	_
			CVE ID : CV	E-2019-	9736				
1234n									
minicms									
N/A	06-03-2019	5.8	MiniCMS 1. admin/post blish&delet delete artic vulnerabilit 2018-1889	t.php?stat e= CSRF t les, a diffe cy than CV	te=pu to erent	N/A		A-123 04041	
			CVE ID : CV	E-2019-	9603				
Airdroid									
Airdroid									
N/A	06-03-2019	7.8	The AirDroithrough 4.2 Android alleattackers to of service (size with a many size sdctl/commercial requests. CVE ID: CV	a.1.6 for ows remo o cause a o service cr multaneo n/lite_aut	ote denial ash) ous h/	N/A		A-AIR- 04041	
CV Scoring Scal (CVSS)	e 0-1 1 pe(s): CSRF- Cross S		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
airdrop_proj	ect				
airdrop					
N/A	15-03-2019	5	The AirDrop application through 2.0 for Android allows remote attackers to cause a denial of service via a client that makes many socket connections through a configured port. CVE ID: CVE-2019-9832	N/A	A-AIR-AIRD- 040419/4
			CVE ID . CVE-2019-9032		
airmore					
airmore					
N/A	15-03-2019	7.8	The AirMore application through 1.6.1 for Android allows remote attackers to cause a denial of service (system hang) via many simultaneous /?Key=PhoneRequestAuth orization requests.	N/A	A-AIR-AIRM- 040419/5
			CVE ID : CVE-2019-9831		
Apache					
jmeter					
N/A	06-03-2019	7.5	Unauthenticated RCE is possible when JMeter is used in distributed mode (-r or -R command line options). Attacker can establish a RMI connection to a jmeter-server using RemoteJMeterEngine and proceed with an attack using untrusted data deserialization. This only affect tests running in	N/A	A-APA-JMET- 040419/6

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CV	E ID	Pa	itch	NCII	PC ID
			Distributed that version are not able traffic between nor authent participating upgrade to also advised CVE ID: CV	ns before to encr een the cicate the g nodes JMeter 5	e 4.0 ypt nodes, e so 5.1 is				
qpid_broker-j									
N/A	06-03-2019	5	A Denial of vulnerability Apache Qpi versions 6.0 (inclusive) allows an unattacker to broker instance specially crommands protocol version (AMQP) and 0-10). Unquid Broke 6.0.0-7.0.6 for 7.1.0 utilizing protocols 0 must up Broker-J version 7.1.1 or late CVE ID : CV	ry was for d Broke 0.0-7.0.6 and 7.1.0 nauthen crash the ance by stance afted using Al using Al rsions b 0-8, 0-9, Jsers of r-J versi (inclusive ing AMQI -8, 0-9, (grade to rsions 7	or-J which ticated e sending MQP elow 0-91 Apache ons re) and P 0-91, 0- Qpid .0.7 or	N/A		A-APA 04041	QPID- 9/7
Solr			T. A. 1. C	-1.	-				
N/A	07-03-2019	7.5	In Apache S 5.0.0 to 5.5. 6.6.5, the Co to configure server via a	5 and 6. onfig AP e the JM	0.0 to I allows X	N/A		A-APA 04041	-SOLR- 9/8
CV Scoring Scale (CVSS) Vulnerability Ty	e 0-1 pe(s): CSRF- Cross		3-4	4-5 Frav Dire	5-6	6-7 ersal; +In	7-8 Ifo- Gain Ir	8-9 nformatio	9-10 n; DoS-
, , ,	Denial of Service				_			2110	

Vulnerability Type(s)	Pı	ublish Da	te	cvss	[Descript	tion & CV	E ID	Pa	atch	NCII	PC ID
					malic attac adva deser remo	cious R ker con ntage o rializat ote cod olr sid		er, an unsafe rigger ion on				
apowersoft					CVE	ID : CV	E-2019	-0192				
apowermana	ger											
N/A		03-201	9	5	appli for A attac of ser simu /?Ke oriza	cation ndroic kers to rvice v ltaneo y=Pho	rManage through allows cause a ia many us neReque equests.	a 3.1.7 remote denial estAuth	N/A		A-APO APOW 04041	<i>7</i> _
appcms												
appcms												
N/A	06-	03-201	9	4.3	XSS v uploa para	via the ad/call ms par).101 all back.ph ameter. 'E-2019	p	N/A		A-APF 04041	P-APPC- 9/10
Apple												
Safari												
N/A	05-	03-201	9	6.8	corru addr mem issue tvOS	essed vory ha	issues w with imp ndling. T d in iOS , Safari 1	oroved This 12.1.3,	N/A		A-APP 04041	P-SAFA- 9/11
CV Scoring Scale (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				_	_	_		ctory Trav njection; N				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description	on & CVE ID	Pa	tch	NCII	PC ID
			Windows, iCl Windows 7.1 maliciously content may arbitrary cod CVE ID : CVE	0. Processing rafted web lead to le execution.				
N/A	05-03-2019	6.8	addressed with memory han issue is fixed tvOS 12.1.2, SiTunes 12.9.3 Windows, iCl Windows 7.1 maliciously content may arbitrary code	dling. This in iOS 12.1.3, Safari 12.0.3, If or oud for 0. Processing crafted web lead to le execution.	N/A		A-APP 04041	-SAFA- 9/12
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6216		ort.ap	//supp ple.co 20945	A-APP 04041	-SAFA- 9/13
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3,		ort.ap	//supp ple.co 20945	A-APP 04041	-SAFA- 9/14
CV Scoring Scal (CVSS)	e 0-1 1-	2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

			Safari 12.0 for Window Windows 7 maliciously	vs, iCloud					
			content ma arbitrary c CVE ID : CV	crafted y lead to ode exect	essing web ution.				
N/A 05-	-03-2019	6.8	Multiple m corruption addressed memory ha issue is fixe tvOS 12.1.2 Safari 12.0 for Windows 7 maliciously content ma arbitrary c	issues w with imp andling. T ed in iOS 2, watchO .3, iTunes vs, iCloud 7.10. Proc y crafted by lead to ode execu	roved This 12.1.3, S 5.1.3, S 12.9.3 If for tessing web ution.	ort.ap	//supp ple.co 20945	A-APP 04041	-SAFA- 9/15
N/A 05-	-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6227			ort.ap	//supp ple.co 20945	A-APP 04041	-SAFA- 9/16
N/A 05-	-03-2019	4.3	A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation.			ort.ap	//supp ple.co 20944	A-APP 04041	-SAFA- 9/17
CV Scoring Scale (CVSS) Vulnerability Type(s):	0-1 1-2		3-4 st Forgery; Dir.	4-5 Trav Dire	5-6	6-7 ersal; +In	7-8 fo- Gain Ir	8-9	9-10 n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			This issue is fixed in iOS 12.1.3, Safari 12.0.3. Processing maliciously crafted web content may lead to a cross site scripting attack. CVE ID: CVE-2019-6228		
N/A	05-03-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processin maliciously crafted web content may lead to universal cross site scripting. CVE ID: CVE-2019-6229	https://supp ort.apple.co m/HT20945 1	A-APP-SAFA- 040419/18
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processin maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6233	https://supp ort.apple.co m/HT20945 1	A-APP-SAFA- 040419/19
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is	https://supp ort.apple.co m/HT20945	A-APP-SAFA- 040419/20
CV Scoring Scal (CVSS)	e 0-1 1-	2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
Vulnerability Ty			st Forgery; Dir. Trav Directory 1 s Site Scripting; Sql- SQL Injection 7		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Icloud			fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6234	1	
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6212	N/A	A-APP-ICLO- 040419/21
N/A	05-03-2019	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6215	N/A	A-APP-ICLO- 040419/22
N/A	05-03-2019	6.8	Multiple memory	https://supp	A-APP-ICLO-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6216	ort.apple.co m/HT20945 1	040419/23
			Multiple memory		
N/A	05-03-2019	6.8	corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	https://supp ort.apple.co m/HT20945	A-APP-ICLO- 040419/24
			CVE ID : CVE-2019-6217 Multiple memory		
N/A	05-03-2019	6.8	corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	https://supp ort.apple.co m/HT20945	A-APP-ICLO- 040419/25

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6226		
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6227	https://supp ort.apple.co m/HT20945 1	A-APP-ICLO- 040419/26
N/A	05-03-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to universal cross site scripting. CVE ID: CVE-2019-6229	https://supp ort.apple.co m/HT20945 1	A-APP-ICLO- 040419/27
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web	https://supp ort.apple.co m/HT20945 1	A-APP-ICLO- 040419/28

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			content may lead to arbitrary code execution. CVE ID: CVE-2019-6233		
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6234	https://supp ort.apple.co m/HT20945	A-APP-ICLO- 040419/29
Itunes					
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6212	N/A	A-APP-ITUN- 040419/30
N/A	05-03-2019	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for	N/A	A-APP-ITUN- 040419/31

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

Vulnerability Type(s)	Publish Date	cvss	Description & CVE II	D Patch	NCIIPC ID
			Windows, iCloud for Windows 7.10. Proces maliciously crafted we content may lead to arbitrary code execution in the content of the code of	on.	
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with impromemory handling. The issue is fixed in iOS 12 tvOS 12.1.2, watchOS Safari 12.0.3, iTunes 1 for Windows, iCloud for Windows 7.10. Process maliciously crafted we content may lead to arbitrary code execution.	e oved is 2.1.3, 5.1.3, 2.9.3 or ssing eb ann.	A-APP-ITUN- 040419/32
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with impromemory handling. The issue is fixed in iOS 12 tvOS 12.1.2, watchOS Safari 12.0.3, iTunes 1 for Windows, iCloud for Windows 7.10. Process maliciously crafted we content may lead to arbitrary code execution.	e ved is 2.1.3, https://supp ort.apple.co m/HT20945 1 sing eb	A-APP-ITUN- 040419/33
N/A	05-03-2019	6.8	An out-of-bounds read addressed with improbounds checking. This issue is fixed in iOS 12 macOS Mojave 10.14.3	ort.apple.co m/HT20945	A-APP-ITUN- 040419/34
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	3-4 4-5	5-6 6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description	& CVE ID	Pa	tch	NCII	PC ID
			iTunes 12.9.3 Windows. A mapplication madelevate privile.	alicious ay be able to ges.				
N/A	05-03-2019	6.8	Multiple memory corruption issuaddressed with memory handle issue is fixed in tvOS 12.1.2, w. Safari 12.0.3, if for Windows, if Windows 7.10 maliciously cracontent may be arbitrary code	h improved ling. This n iOS 12.1.3, atchOS 5.1.3, Tunes 12.9.3 iCloud for . Processing afted web ead to execution.	ort.ap	//supp ple.co 20945	A-APP 04041	-ITUN- 9/35
N/A	05-03-2019	6.8	A memory corrissue was addrimproved membrandling. This fixed in iOS 12 12.1.2, watch C Safari 12.0.3, i'very for Windows, i Windows 7.10 maliciously cracontent may be arbitrary code CVE ID: CVE-2	ort.ap	//supp ple.co 20945	A-APP 04041	9/36	
N/A	05-03-2019	4.3	A logic issue waddressed with validation. Thi fixed in iOS 12 12.1.2, Safari 1 iTunes 12.9.3	ort.ap	//supp ple.co 20945	A-APP 04041	-ITUN- 9/37	
CV Scoring Scale	e 0-1 1-	2 2	3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Da	ate C	vss	Des	criptio	1 & CV	E ID	Pa	atch	NCI	IPC ID
				Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to universal cross site scripting. CVE ID: CVE-2019-6229							
N/A	05-03-201	.9 6.	.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6233				ort.ap	//supp ple.co `20945	A-APF 04041	P-ITUN- 19/38
N/A	05-03-201	.9 6.	.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6234			ort.ap	//supp ple.co `20945	A-APF 04041	P-ITUN- 19/39	
axiosys											
bento4 N/A	01-03-201	9 6	.8	An issue	0.1470.0	diccor	vored in	N/A		ΛΛ	-BENT-
CV Scoring Scal		0.		All ISSU	e was (aisco\	erea III	11/11		A-AAI	-DEN1-
(CVSS)	0-1	1-2 oss Site R			-4 Dir. Tra	4-5 v Dire	5-6 ectory Trav	6-7 versal; +lı	7-8 nfo- Gain II	8-9 nformation	9-10 on; DoS-
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 & CV	E ID	Pa	tch	NCIIPC ID		
			Bento 4 1.5. of bounds we AP4_CttsTableEnd in Core/Ap be triggered crafted file example) the binary. It all attacker to Service (Segfault) or pounspecified CVE ID: CV	write occubleEntry ntry() log 4Array.h d by send to (for he mp42 lows an cause De gmentati ssibly ha l other in	eurs in 7::AP4_ cated a. It can ding a hls enial of ion ave apact.			040419/40		
blog_mini_pro	 oject									
blog_mini										
N/A	14-03-2019	4.3	In Blog_mir via the auth comment reapp/main/articleDetairelated to app/templamments.htm CVE ID: CV	nor name eply in the views.py ils() fund the start attes/_artes/_artes/	e of a ne ction, cicle_co	N/A		A-BLO- BLOG- 040419/41		
bluecms_proj	ect									
bluecms										
N/A	06-03-2019	7.5	BlueCMS 1.6 allows SQL Injection via the user_id parameter in an uploads/admin/user.php? act=edit request. CVE ID: CVE-2019-9594		N/A		A-BLU- BLUE- 040419/42			
bluemind										
bluemind										
CV Scoring Scal (CVSS)	e 0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9 9-1		
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	04-03-2019	5	In BlueMind 3.5.x before 3.5.11 Hotfix 7 and 4.x before 4.0-beta3, the contact application mishandles temporary	N/A	A-BLU- BLUE- 040419/43
			uploads. CVE ID : CVE-2019-9563		
Bolt					
Bolt					
N/A	07-03-2019	6.5	Controller/Async/Filesyst emManager.php in the filemanager in Bolt before 3.6.5 allows remote attackers to execute arbitrary PHP code by renaming a previously uploaded file to have a .php extension. CVE ID: CVE-2019-9185	N/A	A-BOL- BOLT- 040419/44
checkstyle					
checkstyle					
N/A	11-03-2019	5	Checkstyle before 8.18 loads external DTDs by default. CVE ID: CVE-2019-9658	N/A	A-CHE- CHEC- 040419/45
chshcms					
cscms					
N/A	07-03-2019	4.3	An issue was discovered in Cscms 4.1.0. There is an admin.php/pay CSRF vulnerability that can change the payment account to redirect funds. CVE ID: CVE-2019-9598	N/A	A-CHS- CSCM- 040419/46
CV Scoring Scal	0-1 1-		3-4 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					
Cisco										
application_p	olicy_infrastruc	ture_c	ontroller							
N/A	11-03-2019	3.3	A vulnerability in the management interface of Cisco Application Policy Infrastructure Controller (APIC) software could allow an unauthenticated, adjacent attacker to gain unauthorized access on an affected device. The vulnerability is due to a lack of proper access control mechanisms for IPv6 link-local connectivity imposed on the management interface of an affected device. An attacker on the same physical network could exploit this vulnerability by attempting to connect to the IPv6 link-local address on the affected device. A successful exploit could allow the attacker to bypass default access control restrictions on an affected device. Cisco Application Policy Infrastructure Controller (APIC) devices running versions prior to 4.2(0.21c) are affected. CVE ID: CVE-2019-1690		A-CIS-APPL- 040419/47					
enterprise_chat_and_email										
N/A	11-03-2019	4.3	Multiple vulnerabilities in	N/A	A-CIS-ENTE-					
(CVSS)	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; DoSDenial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	itch	NCII	IPC ID
			the web-ba	sed				04041	9/48
			manageme						
			Cisco Enter	_					
			Email could						
			unauthenti						
			attacker to						
			cross-site s		` ,				
			attack agai						
			web-based	•					
			interface of		cted				
			software. T						
			vulnerabili						
			insufficient						
			user-suppl	-	-				
			web-based interface of	•					
			software. A						
					ei				
			could explo vulnerabili		or by				
			injecting m		-				
			a chat wind						
			sending a c	_					
			user of the						
			both cases,						
			must persu						
			click the cr						
			open the cl	at wind	ow that				
			contains th	e attacke	er's				
			code. A suc	cessful e	xploit				
			could allow		-				
			execute arl	itrary so	cript				
			code in the	-	-				
			affected int	erface o	r access				
			sensitive, b	rowser-l	based				
			informatio	n. Versio	n				
			11.6(1) is a	ffected.					
			CVE ID : CV	/E-2019	-1702				
Cleanersoft									
CV Scoring Scale (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cros	_			_				n; DoS-
Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish D	ate	cvss	Descrip	tion & CV	E ID	Pa	itch	NCII	IPC ID
free_mp3_cd_	ripper									
N/A	14-03-201	19	6.8	Stack-base overflow in Ripper 2.6, converting user-assist attackers to arbitrary comp3 file. CVE ID: CVE	N/A		A-CLE 04041	-FREE- 19/49		
N/A	14-03-201	19	6.8	Stack-base overflow in Ripper 2.6, converting user-assist attackers to arbitrary co.wma file. CVE ID : CVE	N/A		A-CLE 04041	-FREE- 19/50		
Cmsmadesim	ple									
cms_made_sii										
N/A	class.showtime2_image.p p in CMS Made Simple (CMSMS) before 2.2.10 does not ensure that a watermark file has a standard image file extension (GIF, JPG, JPEG or PNG). CVE ID: CVE-2019-9692				ple 2.10 at a a JPEG,	N/A		A-CMS 04041	S-CMS 19/51	
N/A	11-03-201	19	6.5	In CMS Made Simple (CMSMS) before 2.2.10, an authenticated user can achieve SQL Injection in class.showtime2_data.php via the functions			N/A		A-CMS 04041	S-CMS 19/52
CV Scoring Scal (CVSS)	0-1	1-2		-3 3-4	4-5	5-6	6-7	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; SqI- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
			_updateshow (parameter show_id), _inputshow (parameter show_id), _Getshowinfo (parameter show_id), _Getpictureinfo (parameter picture_id), _AdjustNameSeq (parameter shownumber), _Updatepicture (parameter picture_id), and _Deletepicture (parameter picture_id). CVE ID : CVE-2019-9693						
codecrafters									
ability_mail_s	erver								
N/A	12-03-2019	4.3	Ability Mail has Persiste Scripting (X body e-mail exploit the the victim remail with Javascript i body of the iframe. CVE ID : CV	ent Cross (SS) via t l body. T vulnerab nust ope maliciou nserted : email as	s Site che che oility, en an as into the	N/A		A-COE 04041	9-ABIL- 9/53
cyberark									
endpoint_priv	vilege_manage	er							
N/A	08-03-2019	6.9	A buffer overflow in the kernel driver CybKernelTracker.sys in CyberArk Endpoint Privilege Manager versions prior to 10.7 allows an attacker (without Administrator		N/A		A-CYB ENDP- 04041	-	
(CVSS)	CV Scoring Scale (CVSS) 1-2 2-3 3-4 4-5 5-6 Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory To					6-7 ersal; +In	7-8 fo- Gain Ir	8-9	9-10 n; DoS-
Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Р	ublish Da	ite	cvss		Descrip	tion & CV	E ID	Pa	atch	NCI	IPC ID
					privileges) to escalate privileges or crash the machine by loading an image, such as a DLL, with a long path.							
					CVI	E ID : CV	E-2019	-9627				
dhcms_projec	ct											
dhcms												
N/A	03-	-03-201	9	3.5	18 l adn /ind	has nin.php? dex XSS		n/Index	N/A		A-DHC DHCM 04042	I -
dilicms												
dilicms												
N/A	07-	-03-201	9	3.5	Dili Stor the sett	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in the first textbox of "System setting->site setting" of admin/index.php, aka			N/A			-DILI- 19/56
					CVI	E ID : CV	E-2019	-8438				
N/A	07-	-03-201	9	3.5	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in the second textbox of "System setting->site setting" of admin/index.php, aka site_domain.		N/A		A-DIL 04042	-DILI- 19/57		
					CVE ID : CVE-2019-8439							
N/A	07	-03-201	9	3.5	An issue was discovered in DiliCMS 2.4.0. There is a Stored XSS Vulnerability in			N/A		A-DIL-DILI- 040419/58		
CV Scoring Scal (CVSS)	е	0-1	1-2	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				_				ectory Trav				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID										
			the third textbox (aka site logo) of "System setting->site setting" of admin/index.php, aka site_logo.																
			CVE ID : CV	E-2019	-8440														
Directadmin																			
Directadmin N/A	07-03-2019	6.8	JBMC Direct allows CSR /CMD_ACC URI to creat account.	F via the OUNT_A te a new	DMIN admin	N/A		A-DIR- 04041											
dradisframev	vork																		
dradis																			
N/A	12-03-2019	3.5	Cross-site scripting vulnerability in Dradis Community Edition Dradis Community Edition v3.11 and earlier and Dradis Professional Edition v3.1.1 and earlier allow remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors. CVE ID: CVE-2019-5925		N/A		A-DRA DRAD- 04041												
ebrigade																			
ebrigade																			
N/A	07-03-2019	4	eBrigade through 4.5 allows Arbitrary File Download via/ directory traversal in the showfile.php file			N/A		A-EBR 04041	-EBRI- 9/61										
CV Scoring Scale (CVSS)	0-1 1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10										
vanierasinty 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		Pa	tch	NCII	PC ID
			parameter, as demonstrated by readi the user- data/save/backup.sql t CVE ID : CVE-2019-96	file.				
editor.md_pro	oject							
editor.md								
N/A	12-03-2019	4.3	Editor.md 1.5.0 has DO based XSS via vectors involving the '					

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			corrupt memory eventually leading to a crash. Only systems offering DTLS connections via APM are impacted. CVE ID: CVE-2019-6596		
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1- 11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/65
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/66

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID		Patch	NCII	IPC ID
			cannot login and does not have the access level to perform the attack.					
			CVE ID : CV	E-2019-6598	3			
N/A	13-03-2019	4.3	In BIG-IP 11.6.1-11.6.3.2 or 11.5.1-11.5.8, or Enterprise Manager 3.1.1, improper escaping of values in an undisclosed page of the configuration utility may result with an improper handling on the JSON response when it is injected by a malicious script via a remote crosssite scripting (XSS) attack.			s://supp 5.com/cs ticle/K4 1178	A-F5-1 04041	
)			
N/A	13-03-2019	4.3	In BIG-IP 14 13.0.0-13.1 12.1.3.7, 11 11.5.1-11.5 remote authenabled for users and a users are grand a users are grandles can be the client vipage. This coross-site seagainst unaclients. CVE ID : CV	e http: ort.fl p/ar 3734	s://supp 5.com/cs ticle/K2 1425	A-F5-1 04041		
big-ip_advanc	ced_firewall_ma	nager					A ===	DIC
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, https://supp ort.f5.com/cs 040419/6					
CV Scoring Scale	e 0-1 1-	2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty	pe(s): CSRF- Cross Sit	_	st Forgery; Dir.	-			nformatio	n; DoS-
	Denial of Service; X	SS- Cross	Site Scripting; 9	SqI- SQL Injection	; N/A- Not	Applicable.		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	p/article/K2 9280193	
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack. CVE ID: CVE-2019-6598	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/70
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/71

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients. CVE ID: CVE-2019-6600		
big-ip_analyti	ics				
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced.	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/72
			CVE ID : CVE-2019-6597		
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/73

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CV	E ID	Pa	itch	NCIII	PC ID
			Configuration lead to disrust services. The requires and user with any than the No The No Accession and logical have the accept of the CVE ID: CV	uption o is attack authent ny role (Access ess user a and do cess leve attack.	f TMUI c icated other role). role es not				
N/A	13-03-2019	4.3	In BIG-IP 14 13.0.0-13.1. 12.1.3.7, 11 11.5.1-11.5. remote authenabled for users and alusers are gr "guest" rolevalues can be the client vipage. This coross-site so against unacclients. CVE ID : CV	ort.f5.	//supp com/cs cle/K2 -25	A-F5-E 04041			
big-ip_applica	l ntion_accelerati	on_ma	nager						
N/A	13-03-2019	6.5	In BIG-IP 13 12.1.0-12.1. 11.6.3.2, or or Enterpris 3.1.1, when administrat commands: Managemen	ort.f5.	//supp com/cs cle/K2 .93	A-F5-E 04041			
CV Scoring Scal	e 0-1 1-	2 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
			referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597 In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-		
N/A	13-03-2019	4	12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack.	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/76
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/77

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

Vulnerability Type(s)	Publish Date	cvss	Description & C\	/E ID	Pa	tch	NCII	PC ID
			page. This can lead cross-site scripting against unauthenti clients.					
			CVE ID : CVE-2019	9-6600				
N/A	13-03-2019	2.1	In BIG-IP 13.0.0, 12 12.1.3.7, 11.6.1-11 11.5.1-11.5.8, the Application Acceler Manager (AAM) was process used in pro- of images and PDFs drop group permis when executing he scripts.	ort.f5.	//supp com/cs cle/K2 02	A-F5-I 04041		
1			CVE ID : CVE-2019	9-6601				
big-ip_appiica	ntion_security_n	nanage	In BIG-IP 13.0.0-13	2111				
N/A	13-03-2019	6.5	12.1.0-12.1.3.7, 11. 11.6.3.2, or 11.5.1- or Enterprise Mana 3.1.1, when authen administrative use commands in the T Management User Interface (TMUI), a referred to as the E Configuration utility restrictions on allo commands may no enforced. CVE ID : CVE-2019	.6.1- 11.5.8 ager ticated rs run raffic also BIG-IP ty, wed t be		•	A-F5-F 04041	
N/A	13-03-2019	4	In BIG-IP 14.0.0-14 13.0.0-13.1.0.7, 12 12.1.3.5, 11.6.1-11 11.5.1-11.5.8 or En	ort.f5.	//supp com/cs cle/K4 00	A-F5-I 04041		
CV Scoring Scale	0							

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)	Pul	blish Da	te	CVSS	·					tch	NCII	PC ID
					requested than have performed by the control of the	nagement erface (Terred to distributed to distributed to distribut	as the B on utility uption consistent authent on Access ess user n and do cess level attack.	ffic Iso IG-IP y, may of TMUI c cicated other role). role es not el to				
N/A	13-0)3-201	9	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients.				ort.f5.	//supp com/cs cle/K2 .25	A-F5-I 04041	
big-ip_domain	n_nar	ne_sys	tem									
N/A	13-0	03-201	9	6.5	12.1 11.6	1.0-12.1 6.3.2, or	3.0.0-13 .3.7, 11. 11.5.1-1 se Mana	6.1- 11.5.8	ort.f5.	//supp com/cs cle/K2 93	A-F5-I 04041	
CV Scoring Scale (CVSS) O-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-												
vuille ability Ty				_				ijection; N				11, 003-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597		
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack.	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/83
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/84

 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
big-ip_edge_g	ateway		users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients. CVE ID: CVE-2019-6600		
0 1- 0 -0			In BIG-IP 13.0.0-13.1.1.1,		
N/A	13-03-2019	6.5	12.1.0-12.1.3.7, 11.6.1- 11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/85
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/86

Vulnerability Type(s)	Pi	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCIII	PC ID
					req use tha The can hav per	vices. The uires and responding the No According the according the according the EID: CV	authent ny role (Access ess user n and do cess leve e attack.	other role). role es not				
N/A	13-	-03-201	9	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients.				ort.f5.	//supp com/cs cle/K2 ·25	A-F5-E 04041	
big-ip_fraud_p	prot	ection_	servi	ice								
N/A	13-	-03-201	9	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1- 11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility,				ort.f5.	//supp com/cs cle/K2 93	A-F5-E 04041	
CV Scoring Scale (CVSS)	е	0-1	1-2	2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597 In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic		
N/A	13-03-2019	4	Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack. CVE ID: CVE-2019-6598	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/89
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/90

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			against unauthenticated clients. CVE ID: CVE-2019-6600		
big-ip_global_	_traffic_manage	r			
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/91
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/92

(CVSS)

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.

3-4

CV Scoring Scale

0-1

1-2

2-3

4-5

5-6

6-7

7-8

8-9

9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			perform the attack. CVE ID: CVE-2019-6598		
N/A 13-03-2019 4.3 big-ip_link_controller		4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients. CVE ID: CVE-2019-6600	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/93
big-ip_link_co	ntroller			1	
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1- 11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/94
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-	https://supp ort.f5.com/cs	A-F5-BIG 040419/95
CV Scoring Scal	e 0-1 1-	2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(CVSS)

Vulnerability Type(s)	Publ	lish Da	te	CVSS	, i					tch	NCII	PC ID
					11.5. Mana request Mana Interpreted to service requirements of the Mana The Mana than	1-11.5 ager 3. ager 3. agement face (To disres and the No According the according to the according t	.8 or Entitle 1.1, male the Train tuser MUI), all as the Bon utility uption on the control of Access ess user and docess leve e attack.	lso IG-IP y, may of TMUI k ticated (other role). role oes not el to	p/arti 46039	cle/K4 00		
N/A	13-03	3-201	9	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients. CVE ID: CVE-2019-6600				ort.f5.	//supp com/cs cle/K2 25	A-F5-I 04041	
big-ip_local_tr	raffic_ı	mana	ger								I	
N/A	13-03	3-201	9	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-				- '	//supp com/cs	A-F5-I 04041	
CV Scoring Scal (CVSS) Vulnerability Ty		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
vanierability Ty				-	_			njection; N				, 503-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	p/article/K2 9280193	
N/A	13-03-2019	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may		https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/98
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/99

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login page. This can lead to a cross-site scripting attack against unauthenticated clients. CVE ID: CVE-2019-6600	ainistrative ternal ed the sanitized flected to e login ead to a ing attack enticated		
big-ip_policy_	enforcement_m	anage	r			
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-BIG 040419/100	
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/101	

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CVE	ID	Pa	tch	NCIII	PC ID
			Configurati lead to disr services. The requires and user with a than the No The No According to the accordin	uption of ais attack authention role (continued authention authent	cated other ole). role				
N/A	13-03-2019	4.3	users are granted the			ort.f5.	//supp com/cs cle/K2 25	A-F5-E 04041	
big-ip_webaco	celerator								
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also			ort.f5.	//supp com/cs cle/K2 93	A-F5-E 04041	
CV Scoring Scale (CVSS)	e 0-1 1-		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
			referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597 In BIG-IP 14.0.0-14.0.0.2,		
N/A	13-03-2019	4	13.0.0-13.1.0.7, 12.1.0- 12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access role). The No Access user role cannot login and does not have the access level to perform the attack. CVE ID: CVE-2019-6598	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-BIG 040419/104
N/A	13-03-2019	4.3	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.3, 12.1.0- 12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when remote authentication is enabled for administrative users and all external users are granted the "guest" role, unsanitized values can be reflected to the client via the login	https://supp ort.f5.com/cs p/article/K2 3734425	A-F5-BIG 040419/105

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			page. This can lead to a cross-site scripting attack against unauthenticated clients.		
			CVE ID : CVE-2019-6600		
enterprise_m	anager		In DIC ID 12 0 0 12 1 1 1	Γ	
N/A	13-03-2019	6.5	In BIG-IP 13.0.0-13.1.1.1, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, when authenticated administrative users run commands in the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, restrictions on allowed commands may not be enforced. CVE ID: CVE-2019-6597	https://supp ort.f5.com/cs p/article/K2 9280193	A-F5-ENTE- 040419/106
N/A	13-03-2019	4	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.0.7, 12.1.0-12.1.3.5, 11.6.1-11.6.3.2, or 11.5.1-11.5.8 or Enterprise Manager 3.1.1, malformed requests to the Traffic Management User Interface (TMUI), also referred to as the BIG-IP Configuration utility, may lead to disruption of TMUI services. This attack requires an authenticated user with any role (other than the No Access user role	https://supp ort.f5.com/cs p/article/K4 4603900	A-F5-ENTE- 040419/107

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CV	E ID	Ра	tch	NCII	PC ID
			cannot logi have the ac perform the						
C : C :			CVE ID : CV						
feifeicms									
feifeicms			FaiFaiCMC	4 1 1002	100	1			
N/A	14-03-2019	7.5	FeiFeiCMS allows remupload and arbitrary Plyvisiting index.php? to modify the allowable finds demonstrated as demonstrated article feat CVE ID: CV	execute execute HP code s=Admin ne set of le exten rated by default peg sett the "add cure.	by n-Index sions, adding ing, and	N/A		A-FEI- 04041	FEIF- 9/108
Fengoffice									
feng_office									
N/A	07-03-2019	7.5	remote atta execute arb " #exec<br .shtml file t ck_upload_)	Feng Office 3.7.0.5 allows remote attackers to execute arbitrary code via " #exec cmd=" in a .shtml file to ck_upload_handler.php.</td <td>N/A</td> <td></td> <td>A-FEN FENG- 04041</td> <td></td>		N/A		A-FEN FENG- 04041	
Ffmpeg			CVE ID : CVE-2019-9623						
Ffmpeg									
N/A	12-03-2019	4.3	In FFmpeg service in the decoder allowed to hog the O	ne subtit ows atta	ile ckers	N/A		A-FFM FFMP- 04041	
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Ty	pe(s): CSRF- Cross S Denial of Service;	_			_				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			crafted video file in Matroska format, because ff_htmlmarkup_to_ass in libavcodec/htmlsubtitles.c has a complex format argument to sscanf. CVE ID: CVE-2019-9718		
N/A	12-03-2019	4.3	A denial of service in the subtitle decoder in FFmpeg 4.1 allows attackers to hog the CPU via a crafted video file in Matroska format, because handle_open_brace in libavcodec/htmlsubtitles.c has a complex format argument to sscanf. CVE ID: CVE-2019-9721	N/A	A-FFM- FFMP- 040419/111
flarumchina					
flarumchina					
N/A	04-03-2019	7.5	FlarumChina v0.1.0- beta.7C has SQL injection via a /?q= request. CVE ID : CVE-2019-9566	N/A	A-FLA-FLAR- 040419/112
Freedesktop					
Poppler					
N/A	01-03-2019	6.8	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readGeneric Bitmap() located in JBIG2Stream.cc, can be triggered by sending a crafted pdf file to (for example) the pdfseparate	N/A	A-FRE-POPP- 040419/113

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCI	IPC ID
			binary. It al attacker to Service (Se fault) or po unspecified This is relat JArithmetic eBit. CVE ID : CV	cause Dogmentat ssibly had other inted to Decoder	ion ave npact. r::decod				
N/A	01-03-2019	6.8	An issue was Poppler 0.7 function car JBIG2Stream ion() located JBIG2Stream triggered by crafted pdf example) the binary. It also attacker to Service (Sefault) or pounspecified This is related JBIG2Bitmated CVE ID : CVE	N/A			C-POPP- 19/114		
N/A	08-03-2019	7.5	Poppler 0.7 based buffer the CairoRed downsamp r function.	N/A			C-POPP- 19/115		
Ftpgetter									
Ftpgetter N/A	13-03-2019	7.5	FTPGetter 5 v.5.97.0.17			N/A			P-FTPG- 19/116
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
vunierability 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. 46								

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CVI	E ID	Pa	tch	NCIII	PC ID
			code execut user initiate connection controlled r sends crafte Long respon crash the F memory con CVE ID : CV						
gitnoteapp			CVL ID . CV	L 2017	7700				
gitnote									
N/A	14-03-2019	6.8	remote atta execute arb a crafted Ma demonstrat javascript:v op.require(.execFile su onerror atta	op.require('child_process') .execFile substring in the onerror attribute of an IMG element.		N/A		A-GIT- 04041	
glyphandcog									
xpdfreader									
N/A	06-03-2019	6.8	There is a stack consumption issue in md5Round1() located in Decrypt.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdfimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.			N/A		A-GLY- 04041	
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	2-3 3-4				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 Da	te CVSS	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
			This is related Catalog::con	ıntPage'					
N/A	06-03-2019	6.8	There is an memory ac gAtomicInc located at G Xpdf 4.01. I triggered by crafted pdf example) the binary. It al attacker to Service (Segfault) or pounspecified CVE ID: CV	N/A			-XPDF- 9/119		
N/A	06-03-2019	6.8	There is a Note of Service (fault) or pounspecified	N/A			-XPDF- 9/120		
Gnome									
N/A	08-03-2019	9 4.3	gio/gsocket			N/A)-GLIB- 9/121
CV Scoring Scale (CVSS)	0-1	1-2 2-3 3-4 4-5 5-6 6-7 cross Site Request Forgery; Dir. Trav Directory Traversal;					7-8	8-9	9-10
vuinerability ly	• • •		st Forgery; Dir. s Site Scripting;		-			iiormatio	II; D05-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			not ensure that a parent GTask remains alive during the execution of a connection-attempting enumeration, which allow remote attackers to cause a denial of service (g_socket_client_connecte _callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany). CVE ID: CVE-2019-9633	ed d	
GNU					
libredwg					
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heap-based buffer overflow in the function dwg_decode_eed_data at decode.c for the y dimension. CVE ID: CVE-2019-9770	N/A	A-GNU-LIBR- 040419/122
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function bit_convert_TU abits.c. CVE ID: CVE-2019-9771	e N/A t	A-GNU-LIBR- 040419/123
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the	N/A	A-GNU-LIBR- 040419/124
CV Scoring Scale (CVSS)	0-1 1-7		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
			function dwg_dxf_LEADER at dwg.spec. CVE ID : CVE-2019-9772		
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heapbased buffer overflow in the function dwg_decode_eed_data at decode.c for the z dimension. CVE ID: CVE-2019-9773	N/A	A-GNU-LIBR- 040419/125
N/A	14-03-2019	6.4	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function bit_read_B at bits.c. CVE ID: CVE-2019-9774	N/A	A-GNU-LIBR- 040419/126
N/A	14-03-2019	6.4	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is an out-of-bounds read in the function dwg_dxf_BLOCK_CONTROL at dwg.spec. CVE ID: CVE-2019-9775	N/A	A-GNU-LIBR- 040419/127
N/A	GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE adwg.spec (later than CVE-2019-9779).		0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (later than CVE-	N/A	A-GNU-LIBR- 040419/128

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heapbased buffer over-read in the function dxf_header_write at header_variables_dxf.spec. CVE ID: CVE-2019-9777	N/A	A-GNU-LIBR- 040419/129
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a heapbased buffer over-read in the function dwg_dxf_LTYPE at dwg.spec. CVE ID: CVE-2019-9778	N/A	A-GNU-LIBR- 040419/130
N/A	14-03-2019	5	An issue was discovered in GNU LibreDWG 0.7 and 0.7.1645. There is a NULL pointer dereference in the function dwg_dxf_LTYPE at dwg.spec (earlier than CVE-2019-9776). CVE ID: CVE-2019-9779	N/A	A-GNU-LIBR- 040419/131
Golang			0121210122013 3773		
GO					
N/A	08-03-2019	6.8	Go through 1.12 on Windows misuses certain LoadLibrary functionality, leading to DLL injection. CVE ID: CVE-2019-9634	N/A	A-GOL-GO- 040419/132
N/A	13-03-2019	4.3	An issue was discovered in net/http in Go 1.11.5. CRLF injection is possible if the attacker controls a	N/A	A-GOL-GO- 040419/133

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	itch	NCIII	PC ID
					der sec http \r\ hea con	parame nonstrat ond argu p.NewRe n follow nder or a nmand.	ed by thument to equest wed by an Redis	o rith 1 HTTP				
golangtc					CV	L ID . CV	E-2019	-9/41				
gopher												
N/A	12	-03-201	9	4.3	DO vec ' <e SRO ' su</e 	jimmykuu Gopher 2.0 has DOM-based XSS via vectors involving the '						

Vulnerability Type(s)	Publish Date	cvss	Description	on & CVE ID	Pa	tch	NCII	PC ID
			to embed ark JavaScript co UI thus alter intended fun potentially le credentials d within a trus IBM X-Force	ripting. This vallows users bitrary ode in the Web ing the actionality eading to disclosure sted session.		t/docvi s?uid=i 37424		
N/A	05-03-2019	3.5	IBM Sterling Integrator 5. 6.0.0.0 is vul cross-site scr vulnerability to embed ark JavaScript co UI thus alter intended fun potentially le credentials d within a trus IBM X-force	B2B 2.0.1 through nerable to ripting. This vallows users bitrary ode in the Web ing the actionality eading to disclosure sted session.	uppor	.com/s t/docvi s?uid=i		-STER- 9/137
N/A	05-03-2019	4.3	IBM Sterling Integrator 5. 6.0.0.0 Stand could allow be sensitive information the middle IBM X-Force CVE ID : CVE	uppor	.com/s t/docvi s?uid=i		-STER- 9/138	
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	[Descript	ion & CV	E ID	Pa	tch	NCIII	PC ID
websphere_a	pplication_serv	er								
N/A	06-03-2019	3.5	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155946.				N/A		A-IBM WEBS- 04041	-
			CVE	ID : CV	E-2019	-4030				
websphere_vi	irtual_enterpris	e								
N/A	06-03-2019	3.5	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross- site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155946. CVE ID: CVE-2019-4030				N/A		A-IBM WEBS- 04041	-
financial_tran	saction_manag	er								
N/A	05-03-2019	7.5	IBM Financial Transaction Manager for Digital Payments for Multi- Platform 3.1.0 is vulnerable to SQL				N/A		A-IBM-FINA- 040419/141	
CV Scoring Scale (CVSS)	e 0-1 1-	2 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 Dat	e CVSS	Descrip	tion & CVI	ID	Pa	tch	NCI	IPC ID
			injection. A attacker co specially-createments allow the a add, modify information end databa ForceID: 15	uld send rafted SQ , which c ttacker to y or delet n in the b se. IBM X	ould o view, e ack-				
			CVE ID : CV	/E-2019-	4032				
content_navig	ator								
N/A	14-03-2019	6.5	IBM Conter 3.0CD is co attacker to arbitrary co workstatio an executal with Edit se executed or workstatio ID: 156000 CVE ID: CV	uppor ew.ws	//ww .com/s t/docvi s?uid=i 86906	A-IBM CONT 04041			
DB2									
N/A	11-03-2019		IBM DB2 for and Windo DB2 Conne 10.1, 10.5, a vulnerable overflow, wallow an authocal attack arbitrary consystem as a ForceID: 15 CVE ID: CVE	uppor ew.ws bm10	.com/s t/docvi s?uid=i 74041	04041	I-DB2- 19/143		
CV Scoring Scale		7.2	IBM DB2 fo	https:	//ww	A-IBM-DB2-			
(CVSS) Vulnerability Typ	pe(s): CSRF- Cro	ss Site Reque	st Forgery; Dir. s Site Scripting;		_			8-9 nformatio	9-10 on; DoS-

Vulnerability Type(s)	Publish Dat	e CVSS	Descript	tion & CV	E ID	Pa	tch	NCII	PC ID		
			and Windown DB2 Conne 10.1, 10.5, a vulnerable overflow, wallow an aulocal attack arbitrary consystem as referee ID: 15	uppor	.com/s t/docvi s?uid=i 74041	04041	9/144				
			CVE ID : CV	/E-2019	-4016						
insurance_wallet											
insurance_wa	illet		<u> </u>			ı		ı			
N/A	12-03-2019	5	vulnerabilit Insurance V iOS Version earlier allov attackers to files via uns vectors.	Directory traversal vulnerability in iChain Insurance Wallet App for iOS Version 1.3.0 and earlier allows remote attackers to read arbitrary files via unspecified vectors. CVE ID: CVE-2019-5923				A-ICH- 04041	-INSU- 9/145		
Imagemagick											
Imagemagick											
N/A	07-03-2019	5	In ImageMa 7.0.8-25, so leaks exist i in coders/p CVE ID : CV	ome men in Decod ocd.c.	nory eImage	N/A	A-IMA-IM 040419/1				
Intel											
matrix_storag	ge_manager										
N/A	14-03-2019	4.6	Improper permissions in Intel(R) Matrix Storage Manager 8.9.0.1023 and before may allow an		https://ww w.intel.com/ content/ww w/us/en/sec		A-INT- MATR- 040419/147				
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Ty		-	st Forgery; Dir. s Site Scripting;		-			nformatio	n; DoS-		

Vulnerability Type(s)	P	ublish Da	te	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID
					authentica potentially escalation local acces CVE ID : C	enable of privile s.	ege via	urity- center ory/IN SA- 00216			
usb_3.0_creat	or_u	ıtility									
N/A	14-	-03-2019	9	4.6	Improper y Intel(R) US Utility all v allow an au user to pot escalation local acces CVE ID : C	conter w/us/ urity-	l.com/ nt/ww en/sec /advis VTEL-	A-INT 04041	-USB 9/148		
rapid_storage	_tec	chnology	y_ent	terpris	se						
N/A	14-	-03-2019	9	4.6	the installed Accelerate Manager in before may authentical potentially escalation	Improper permissions in the installer for Intel(R) Accelerated Storage Manager in RSTe v5.5 and before may allow an authenticated user to potentially enable escalation of privilege via local access.		https://ww w.intel.com/ content/ww w/us/en/sec urity- center/advis ory/INTEL- SA- 00231.html			-RAPI- 9/149
iotivity											
iotivity										1	
N/A	13-	-03-2019	9	6.4	In IoTivity through 1.3.1, the CoAP server interface can be used for Distributed Denial of Service attacks using source IP address spoofing and UDP-based traffic amplification. The reflected traffic is 6 times		N/A		A-IOT-IOT: 040419/1		
CV Scoring Scale (CVSS)		0-1	1-2		-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				=	st Forgery; Dir. Site Scripting		=			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CV	E ID	Pa	itch	NCII	PC ID			
			bigger than requests. The because the of a "4.01 U response is NOTE: the way with the work of the control of th	nis occur e constru nauthor mishan vendor s is an attack, t maintai e migra e."	rs action ized" dled. tates here is ner to ting to							
Jenkins script_security												
N/A	08-03-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Script Security Plugin 1.53 and earlier in src/main/java/org/jenkin sci/plugins/scriptsecurity /sandbox/groovy/Groovy Sandbox.java, src/main/java/org/jenkin sci/plugins/scriptsecurity /sandbox/groovy/SecureG roovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM. CVE ID: CVE-2019- 1003029		ns.io/s y/adv 019-0 06/#S TY-	//jenki securit isory/2 3- SECURI %20(1)	A-JEN- 04041					
pipeline_groon	08-03-2019	6.5	A sandbox l vulnerabilit Jenkins Pip	https://jenki ns.io/securit y/advisory/2		A-JEN- 04041						
CV Scoring Scal (CVSS) Vulnerability Ty	e 0-1 1- rpe(s): CSRF- Cross Si Denial of Service;)	te Reque	2-3 3-4 sst Forgery; Dir.	4-5 Trav Dire	5-6	6-7 ersal; +In	7-8 Ifo- Gain Ir	8-9 nformatio	9-10 n; DoS-			

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkin sci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM.	019-03- 06/#SECURI TY- 1336%20(2)	
			CVE ID : CVE-2019- 1003030		
groovy					
N/A	08-03-2019 6.5		A sandbox bypass vulnerability exists in Jenkins Groovy Plugin 2.1 and earlier in pom.xml, src/main/java/hudson/pl ugins/groovy/StringScript Source.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM. CVE ID: CVE-2019- 1003033	https://jenki ns.io/securit y/advisory/2 019-03- 06/#SECURI TY-1338	A-JEN-GR00- 040419/153
matrix_proje	ct				
N/A			A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/m atrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code	https://jenki ns.io/securit y/advisory/2 019-03- 06/#SECURI TY-1339	A-JEN- MATR- 040419/154

Vulnerability Type(s)	Pu	ıblish Da	ite	cvss		Descript	tion & CV	E ID	Pa	itch	NCII	IPC ID
					CVE	,	ins mas [,] / E-201 9	,				
email_extensi	ion								ı		ı	
N/A	08-	03-201	9	6.5	vuln Jenk Plug pon src/ ugin nten src/ ugin nten src/ ugin igge r.jav with per arbid Jenk CVI	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/pl ugins/emailext/ExtendedE mailPublisher.java, src/main/java/hudson/pl ugins/emailext/plugins/co ntent/EmailExtScript.java, src/main/java/hudson/pl ugins/emailext/plugins/co ntent/ScriptContent.java, src/main/java/hudson/pl ugins/emailext/plugins/tr igger/AbstractScriptTrigge r.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM. CVE ID: CVE-2019-1003032				//jenki securit isory/2 3- SECURI 40	1	-EMAI- 19/155
job_dsl	1											
N/A	08-	03-201	9	6.5	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in job-dsl- core/src/main/groovy/jav aposse/jobdsl/dsl/Abstrac tDslScriptLoader.groovy, job-dsl-			ns.io/s y/adv 019-0	SECURI	1	-JOB 19/156	
CV Scoring Scale (CVSS) Vulnerability Ty		0-1 CSRF- Cro	1-2 oss Site		:-3 st Forg	3-4 gery; Dir.	4-5 Trav Dire	5-6 ectory Trav	6-7 ersal; +In	7-8 Ifo- Gain Ir	8-9	9-10 on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			plugin/build.gradle, jobdsl- plugin/src/main/groovy/j avaposse/jobdsl/plugin/Jo bDslWhitelist.groovy, jobdsl- plugin/src/main/groovy/j avaposse/jobdsl/plugin/S andboxDslScriptLoader.gr oovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM. CVE ID: CVE-2019-		
250,000,000	n to		1003034		
N/A	08-03-2019	4	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/micro soft/azure/vmagent/Azur eVMAgentTemplate.java, src/main/java/com/micro soft/azure/vmagent/Azur eVMCloud.java that allows attackers with Overall/Read permission to perform the 'verify configuration' form validation action, thereby obtaining limited information about the Azure configuration. CVE ID: CVE-2019-1003035	https://jenki ns.io/securit y/advisory/2 019-03- 06/#SECURI TY-1330	A-JEN-AZUR- 040419/157

Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
N/A	08-03-2019	4	A data modification vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/micro soft/azure/vmagent/Azur eVMAgent.java that allows attackers with Overall/Read permission to attach a public IP address to an Azure VM agent. CVE ID: CVE-2019-	nkins Azure VM Agents ugin 0.8.0 and earlier in c/main/java/com/micro oft/azure/vmagent/Azur VMAgent.java that allows tackers with verall/Read permission attach a public IP ddress to an Azure VM gent. VE ID: CVE-2019-			
			1003036				
N/A	08-03-2019	4	An information exposure vulnerability exists in Jenkins Azure VM Agents Plugin 0.8.0 and earlier in src/main/java/com/micro soft/azure/vmagent/Azur eVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. CVE ID: CVE-2019-1003037	https://jenki ns.io/securit y/advisory/2 019-03- 06/#SECURI TY-1332	A-JEN-AZUR- 040419/159		
repository_com	nnector						
N/A	08-03-2019	2.1	An insufficiently protected credentials vulnerability exists in Jenkins Repository Connector Plugin 1.2.4 and earlier in src/main/java/org/jvnet/hudson/plugins/repositor yconnector/ArtifactDeploy	https://jenki ns.io/securit y/advisory/2 019-03- 06/#SECURI TY-958	A-JEN-REPO- 040419/160		
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		

appdynamics			er.java, src/main/java/ hudson/plugin: yconnector/Re a, src/main/java/ hudson/plugin: yconnector/Use that allows an a with local file sy access or contre Jenkins adminis web browser (e malicious exter retrieve the pas stored in the pl configuration. CVE ID : CVE-2 1003038 An insufficientl	s/repositor pository.jav /org/jvnet/ s/repositor erPwd.java attacker ystem ol of a strator's e.g. nsion) to ssword ugin				
appdynamics								
арриунаннся			An insufficientl				<u> </u>	
N/A 08-03	-2019 4	ł	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecen tric/jenkins/appd/AppDy namicsResultsPublisher.ja va that allows attackers without permission to obtain passwords configured in jobs to obtain them. CVE ID: CVE-2019-1003039		ns.io/s y/advi 019-03	ECURI	A-JEN- 04041	
Joomla								
CV Scoring Scale (CVSS)	0-1 1-2	2-:	3 3-4 4	-5 5-6				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
Joomla!						
N/A	12-03-2019	4.3	An issue was discovered in Joomla! before 3.9.4. The item_title layout in edit views lacks escaping, leading to XSS. CVE ID: CVE-2019-9711	N/A	A-J00-J00M- 040419/162	
N/A	12-03-2019	4.3	An issue was discovered in Joomla! before 3.9.4. The JSON handler in com_config lacks input validation, leading to XSS. CVE ID: CVE-2019-9712	N/A	A-J00-J00M- 040419/163	
N/A	12-03-2019	5	An issue was discovered in Joomla! before 3.9.4. The sample data plugins lack ACL checks, allowing unauthorized access.	N/A	A-J00-J00M- 040419/164	
			CVE ID: CVE-2019-9713 An issue was discovered in			
N/A	12-03-2019	4.3	Joomla! before 3.9.4. The media form field lacks escaping, leading to XSS.	N/A	A-J00-J00M- 040419/165	
			CVE ID: CVE-2019-9714			
jtbc						
jtbc_php	,					
N/A	11-03-2019	6.4	An issue was discovered in JTBC(PHP) 3.0.1.8. Its cache management module is flawed. An arbitrary file ending in "inc.php" can be deleted via a console/cache/manage.ph p?type=action&action=bat	N/A	A-JTB-JTBC- 040419/166	
CV Scoring Scal	e 0-1 1-	2 2	3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	
(CVSS) Vulnerability Ty			st Forgery; Dir. Trav Directory Trave			

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ch&batch=delete&ids=/ substring. CVE ID : CVE-2019-9662		
kartatopia					
piluscart					
N/A	14-03-2019	6.8	PilusCart 1.4.1 is vulnerable to index.php?module=users& action=newUser CSRF, leading to the addition of a new user as administrator. CVE ID: CVE-2019-9769	N/A	A-KAR-PILU- 040419/167
Korenix					
jetport_web_r	nanager				
N/A	12-03-2019	4.3	The Web manager (aka Commander) on Korenix JetPort 5601 and 5601f devices has Persistent XSS via the Port Alias field under Serial Setting. CVE ID: CVE-2019-9725	N/A	A-KOR-JETP- 040419/168
libofx_project	-				
libofx					
N/A	11-03-2019	6.8	An issue was discovered in LibOFX 0.9.14. There is a NULL pointer dereference in the function OFXApplication::startElem ent in the file lib/ofx_sgml.cpp, as demonstrated by ofxdump. CVE ID: CVE-2019-9656	N/A	A-LIB-LIBO- 040419/169
maccms					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CV33)										

Vulnerability Type(s)	Publish D	ate	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
maccms											
N/A	14-03-203	19	6.5	attacarbirente templorente occurrence oper which problem	ckers to trary PI ering this plate/d Edit acurs becare dering uration out to by panibition plates.	allows rexecuted a second in the second in t	by n a c/html is plate nclude e file, files as	N/A		A-MACC MACC 04041	
Mailtraq											
webmail											
N/A	12-03-203	19	4.3	2.17 Cross via t mess vuln mus mali inse the e	Mailtraq WebMail version 2.17.7.3550 has Persistent Cross Site Scripting (XSS) via the body of an e-mail message. To exploit the vulnerability, the victim must open an email with malicious Javascript inserted into the body of the email as an iframe. CVE ID: CVE-2019-9558					A-MAI WEBM 04041	
Mcafee											
database_sect	urity										
N/A	12-03-203	19	2.1	Data Leakage Attacks vulnerability in the web interface in McAfee Database Security prior to the 4.6.6 March 2019 update allows local users to expose passwords via				cafee.d rporat x?page	//kc.m com/co ce/inde e=cont d=SB10	A-MCA DATA- 04041	
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 Ty	pe(s): CSRF- C Denial of Se		_	_	_		_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	itch	NCII	PC ID			
			incorrectly completing fields in the browser lo	passwo: admin								
			CVE ID : CV	E-2019	-3615							
medical_store	_script_project											
medical_store	_script											
N/A	06-03-2019	5	PHP Scripts Store Scrip Path Trave navigating directory o file. CVE ID : CV	t 3.0.3 al rsal by to the pa f a jpg or	rent png	N/A		A-MEI MEDI- 04041				
Microsoft			CVE ID : CV	E-2019	-9607							
Excel												
Excei			A . C	1.	1	1		T				
N/A	05-03-2019	4.3	An information vulnerability Microsoft Elements of aka 'Microsoft Information Vulnerability vulnerab	ty exists xcel disclose its mem oft Exce n Disclos	when es the ory,	al.msr osoft.c	•		-EXCE- 9/174			
			CVE ID : CV	E-2019	-0669							
excel_viewer												
N/A	05-03-2019	4.3	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs.An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka 'Microsoft Office Security			al.msr osoft.c	•		-EXCE- 9/175			
CV Scoring Scale (CVSS)	0-1 1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10			
Vulnerability Typ	pe(s): CSRF- Cross Si Denial of Service; 3	_	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-									

Vulnerability Type(s)	Pul	blish Da	ite	cvss		Descript	ion & CV	Æ ID	Pa	ntch	NCI	IPC ID
					Vuln	ure Byj ierabili ID : CV		0-0540				
N/A	05-0)3-201	9	4.3	vuln Micr impi cont aka ' Info	erabilit osoft E roperly ents of Micros	disclose its ment oft Excent Disclose	when es the nory,	al.msr osoft.c -US/so guidan	//port rc.micr com/en ecurity- nce/ad r/CVE- 0669		C-EXCE- 19/176
CC 0.4	_				CVE	ID : CV	E-2019)-0669				
office_365_pr	oplus	5			1 A	•• •	1					
N/A	05-0	03-201	9	4.3	vuln Micr valid coul spec coul ente 'Mic Feat Vuln	erabilite osoft C date UR d send cially cr d trick ring cre rosoft (ure By nerabili	the victi edential Office Se pass	when es not ttacker a e, which im into s, aka ecurity	al.msr osoft.c -US/so guidan	//port rc.micr com/en ecurity- nce/ad r/CVE- 0540	A-MI(()++1	
N/A	05-0)3-201	9	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. CVE ID: CVE-2019-0669				al.msr osoft.c -US/so guidan	//port rc.micr com/en ecurity- nce/ad r/CVE- 0669		C-OFFI- 19/178
N/A	05-0)3-201	9	9.3			ode exec y exists			//port c.micr	A-MIC-OFFI-	
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 Ty				_	_	_		ectory Trav njection; N			nformatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019- 0672, CVE-2019-0673, CVE-2019-0674, CVE- 2019-0675. CVE ID: CVE-2019-0671	osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0671	040419/179
N/A	05-03-2019	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675. CVE ID: CVE-2019-0672		https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0672	A-MIC-OFFI- 040419/180
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0673	A-MIC-OFFI- 040419/181

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0674, CVE-2019-0675.		
			CVE ID : CVE-2019-0673		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0673, CVE-2019-0675. CVE ID: CVE-2019-0674	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0674	A-MIC-OFFI- 040419/182
powerpoint_v	viewer				
N/A	05-03-2019	4.3	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs. An attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka 'Microsoft Office Security Feature Bypass Vulnerability'. CVE ID: CVE-2019-0540	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0540	A-MIC- POWE- 040419/183
word_viewer			CVE ID . CVE-2019-0340		
N/A	05-03-2019	4.3	A security feature bypass	https://port	A-MIC-
CV Scoring Scal	e			1 111	
(CVSS)	pe(s): CSRF- Cross Sit	e Reque	st Forgery; Dir. Trav Directory Traves Site Scripting; Sql- SQL Injection; N/		8-9 9-10 formation; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CVI	E ID	Pa	tch	NCII	PC ID
chakracore			vulnerabilimicrosoft Coalidate UR could send specially creature By Vulnerabilic CVE ID : CV	Office doe Ls.An att a victim afted file the victin edentials Office Sec pass ty'.	s not cacker a , which in into c, aka curity	-US/se	com/en ecurity- nce/ad /CVE-	WORE 04041)- .9/184
CHAIN ACUIC			A romoto o	ada ayaa	ıtion				
N/A	05-03-2019	7.6	A remote covulnerability way that the engine hand memory in aka 'Scripti Memory Covulnerabilitis unique fro 0591, CVE-2019-0610, CVE-2019-0644, CVE-2019-0651, CVE-2019-CVE-20	-US/se guidar visory 2019-	c.micr com/en ecurity- nce/ad /CVE- 0590	A-MIC CHAK- 04041			
N/A	05-03-2019	7.6	A remote convulnerability way that the engine hand memory in aka 'Scripti Memory Co	-US/se	c.micr com/en ecurity- nce/ad /CVE-	A-MIC CHAK- 04041			
CV Scoring Scale (CVSS)	0-1	1-2	2-3 3-4	6-7	7-8	8-9	9-10		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0591		
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0593	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0593	A-MIC- CHAK- 040419/187
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0605	A-MIC- CHAK- 040419/188

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0607, CVE-2019-0610, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0605		
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0607	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0607	A-MIC- CHAK- 040419/189
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0610	A-MIC- CHAK- 040419/190

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			0590, CVE-2019-0591, CVE-2019-0593, CVE- 2019-0605, CVE-2019- 0607, CVE-2019-0640, CVE-2019-0642, CVE- 2019-0644, CVE-2019- 0651, CVE-2019-0652, CVE-2019-0655.		
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0655. CVE ID: CVE-2019-0640	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0640	A-MIC- CHAK- 040419/191
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0642	A-MIC- CHAK- 040419/192

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0642		
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0644	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0644	A-MIC- CHAK- 040419/193
N/A	05-03-2019	6.8	A vulnerability exists in Microsoft Chakra JIT server, aka 'Scripting Engine Elevation of Privileged Vulnerability'. CVE ID: CVE-2019-0649	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0649	A-MIC- CHAK- 040419/194
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in	https://port al.msrc.micr osoft.com/en -US/security-	A-MIC- CHAK- 040419/195

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0651	guidance/ad visory/CVE- 2019-0651	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0655. CVE ID: CVE-2019-0652	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0652	A-MIC- CHAK- 040419/196
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad	A-MIC- CHAK- 040419/197

Vulnerability Type(s)	Publish Dat	te CVSS	Descript	tion & CV	E ID	Pa	atch	NCII	PC ID
			Vulnerabili is unique fr 0590, CVE- CVE-2019-0 2019-0605 0607, CVE- CVE-2019-0 2019-0642 0644, CVE- CVE-2019-0	Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019- 0590, CVE-2019-0591, CVE-2019-0593, CVE- 2019-0605, CVE-2019- 0607, CVE-2019-0610, CVE-2019-0640, CVE- 2019-0642, CVE-2019- 0644, CVE-2019-0651, CVE-2019-0652. CVE ID: CVE-2019-0655					
N/A	05-03-2019	4.3	An informa vulnerability the scripting not properly objects in manda objects in manda of the control of the con	ty exists g engine y handle nemory dge, aka ngine n Disclos ty'. This om CVE	when e does in sure CVE ID -2019-	al.msr osoft.c -US/so guidan	//port c.micr com/en ecurity- nce/ad r/CVE- 0658	A-MIC CHAK 04041	
sharepoint_se	erver								
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0604.			al.msr osoft.c -US/so guidan	//port rc.micr com/en ecurity- nce/ad r/CVE- 0594		-SHAR- .9/199
CV Scoring Scale (CVSS) Vulnerability Ty	0-1		2-3 3-4 st Forgery; Dir.	4-5 Trav Dire	5-6 ectory Trav	6-7 ersal; +Ir	7-8 nfo- Gain Ir	8-9	9-10
, ,		_	Site Scripting;		_				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594. CVE ID: CVE-2019-0604	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0604	A-MIC-SHAR- 040419/200
sharepoint_e	nterprise_serve	r			
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0604. CVE ID: CVE-2019-0594	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0594	A-MIC-SHAR- 040419/201
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0604	A-MIC-SHAR- 040419/202

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			0594. CVE ID : CVE-2019-0604		
N/A	05-03-2019	6.5	An elevation of privilege vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft SharePoint Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0668	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0668	A-MIC-SHAR- 040419/203
N/A	05-03-2019	5.8	A spoofing vulnerability exists in Microsoft SharePoint when the application does not properly parse HTTP content, aka 'Microsoft SharePoint Spoofing Vulnerability'. CVE ID: CVE-2019-0670	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0670	A-MIC-SHAR- 040419/204
sharepoint_fo	oundation		CVE ID . CVE-2019-0070		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0604. CVE ID: CVE-2019-0594	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0594	A-MIC-SHAR- 040419/205

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in Microsoft SharePoint when the software fails to check the source markup of an application package, aka 'Microsoft SharePoint Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0594. CVE ID: CVE-2019-0604	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0604	A-MIC-SHAR- 040419/206
N/A	05-03-2019	5.8	A spoofing vulnerability exists in Microsoft SharePoint when the application does not properly parse HTTP content, aka 'Microsoft SharePoint Spoofing Vulnerability'. CVE ID: CVE-2019-0670	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0670	A-MIC-SHAR- 040419/207
internet_expl	orer				
N/A	05-03-2019	7.6	A remote code execution vulnerability exists when Internet Explorer improperly accesses objects in memory, aka 'Internet Explorer Memory Corruption Vulnerability'. CVE ID: CVE-2019-0606	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0606	A-MIC-INTE- 040419/208
N/A	05-03-2019	4.3	A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects, aka 'Microsoft Browser Spoofing Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-	A-MIC-INTE- 040419/209

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0654	2019-0654	
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when Internet Explorer improperly handles objects in memory. An attacker who successfully exploited this vulnerability could test for the presence of files on disk, aka 'Internet Explorer Information Disclosure Vulnerability'. CVE ID: CVE-2019-0676	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0676	A-MIC-INTE- 040419/210
.net_framewo	rk				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file.An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework and Visual Studio Remote Code Execution Vulnerability'. CVE ID: CVE-2019-0613	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0613	A-MICNET- 040419/211
N/A	05-03-2019	4.3	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-	A-MICNET- 040419/212

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'.	2019-0657	
			CVE ID: CVE-2019-0657		
visual_studio_	2017				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in .NET Framework and Visual Studio software when the software fails to check the source markup of a file.An attacker who successfully exploited the vulnerability could run arbitrary code in the context of the current user, aka '.NET Framework and Visual Studio Remote Code Execution Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0613	A-MIC-VISU- 040419/213
			CVE ID : CVE-2019-0613		
N/A	05-03-2019	4.3	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing Vulnerability'. CVE ID: CVE-2019-0657	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0657	A-MIC-VISU- 040419/214
powershell_co	ore				
N/A	05-03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0627	A-MIC- POWE- 040419/215
CV Scoring Scale (CVSS)	0-1 1-		3-4 4-5 5-6 st Forgery; Dir. Trav Directory Trave	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publis	h Date	cvss		Descript	ion & CV	E ID	Pa	itch	NCII	PC ID
				201	9-0632						
				CVI	E ID : CV	E-2019	-0627				
N/A 05-03-2019			4.6	allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from				al.msr osoft.c -US/se guidan	//port c.micr com/en ecurity- nce/ad r/CVE- 0631	A-MIC POWE 04041	
				CVI	E ID : CV	E-2019	-0631				
N/A	05-03-	2019	4.6	vuli Wir allo byp 'Wir Byp CVE CVE 201	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0631.			al.msr osoft.c -US/se guidar	//port cc.micr com/en ecurity- nce/ad r/CVE- 0632	A-MIC POWE 04041	
N/A	05-03-	2019	4.3	cert API the aka Visu Vul	A vulnerability exists in certain .Net Framework API's and Visual Studio in the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing Vulnerability'. CVE ID: CVE-2019-0657		al.msr osoft.c	•	A-MIC POWE 04041		
.net_core											
N/A	05-03-	2019	4.3	cert	A vulnerability exists in certain .Net Framework API's and Visual Studio in		https://port al.msrc.micr osoft.com/en			NET- .9/219	
CV Scoring Scal (CVSS)	e 0-	1 1	-2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty			-				ctory Trav			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the way they parse URL's, aka '.NET Framework and Visual Studio Spoofing Vulnerability'. CVE ID: CVE-2019-0657	-US/security- guidance/ad visory/CVE- 2019-0657	
office_compat	tibility_pack		000101010101007		
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when Microsoft Excel improperly discloses the contents of its memory, aka 'Microsoft Excel Information Disclosure Vulnerability'. CVE ID: CVE-2019-0669	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0669	A-MIC-OFFI- 040419/220
exchange_ser	ver				
N/A	05-03-2019	5.8	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0724. CVE ID: CVE-2019-0686	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0686	A-MIC-EXCH- 040419/221
N/A	05-03-2019	9.3	An elevation of privilege vulnerability exists in Microsoft Exchange Server, aka 'Microsoft Exchange Server Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0686. CVE ID: CVE-2019-0724	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0724	A-MIC-EXCH- 040419/222
visual_studio_	_code				

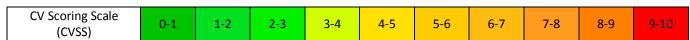
 CV Scoring Scale (CVSS)
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7
 7-8
 8-9
 9-10

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID	Pa	tch	NCIII	PC ID
N/A	05-03-2019	9.3	vulnerabilit Visual Studi process env variables af project, aka Code Remo Execution V	io Code when i vironment ter opening a 'Visual Studio	al.msr osoft.c -US/se guidar visory 2019-	com/en ecurity- nce/ad /CVE-	A-MIC- 04041	
java_software	e_development_	kit						
N/A	05-03-2019	7.5	vulnerabilit way Azure l generates sy for encrypti attacker to y randomnes aka 'Azure l Elevation of Vulnerabilit	s of the key, oT Java SDK f Privilege	osoft.c -US/se guidar visory 2019-	c.micr com/en ecurity- nce/ad /CVE-	A-MIC- 04041	-
N/A	05-03-2019	5	vulnerabilit way Azure l logs sensitiv aka 'Azure l Information Vulnerabilit		https:, al.msr osoft.c -US/se guidan visory 2019-	com/en ecurity- nce/ad /CVE-	A-MIC- 04041	•
team_foundat	tion_server							
N/A	05-03-2019	3.5	when Team	rability exists Foundation not properly r provided	-US/se	c.micr com/en ecurity- nce/ad	A-MIC- TEAM- 04041	
CV Scoring Scale (CVSS)	e 0-1 1-		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
			Foundation Server Cross- site Scripting Vulnerability'. This CVE I is unique from CVE-2019 0743. CVE ID: CVE-2019-0742	D -	
N/A	05-03-2019	3.5	A Cross-site Scripting (XSS) vulnerability exists when Team Foundation Server does not properly sanitize user provided input, aka 'Team Foundation Server Cross- site Scripting Vulnerability'. This CVE II is unique from CVE-2019 0742. CVE ID: CVE-2019-0743	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0743	A-MIC- TEAM- 040419/227
teams					
N/A	12-03-2019	6.8	Untrusted search path vulnerability in The installer of Microsoft Teams allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory. CVE ID: CVE-2019-5922	N/A	A-MIC- TEAM- 040419/228
Office					
N/A	05-03-2019	4.3	A security feature bypass vulnerability exists when Microsoft Office does not validate URLs. An attacked could send a victim a specially crafted file, which could trick the victim into entering credentials, aka	al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-	A-MIC-OFFI- 040419/229
CV Scoring Scal (CVSS)	0-1		2-3 3-4 4-5 5-6 st Forgery; Dir. Trav Directory T	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Da	ote CVSS	5	Descript	ion & CV	E ID	Pa	tch	NCII	IPC ID
			Fea	crosoft (ature By _l Inerabili	pass	curity				
			CV.	E ID : CV	E-2019	-0540				
N/A	05-03-201	9 4.3	vul Mid imp cor aka Info	informanerabiliterosoft Eproperly atents of a 'Microsormation Inerabilite ID: CV	ty exists xcel disclose its mem oft Exce n Disclosety'.	when es the ory, l sure	al.msr osoft.c	com/en ecurity- nce/ad /CVE-		C-OFFI- 19/230
N/A	05-03-201	9 9.3	vul the Cor imp obj 'Mi Cor Rer Vul is v 06% CVI 20%	emote connerability of the connectivity of the	ey exists oft Office y Engine handles nemory, Office Ac y Engine ty'. This om CVE 2019-06	when Access aka cess tion CVE ID -2019- 73,	al.msr osoft.c	com/en ecurity- nce/ad /CVE-		-OFFI- 19/231
N/A	05-03-201	9 9.3	vul the Cor imp obj 'Mi Cor	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution			al.msr osoft.c	com/en ecurity- nce/ad /CVE-		:-OFFI- 19/232
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cr Denial of Ser	-				_			ntormatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675. CVE ID: CVE-2019-0672		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0674, CVE-2019-0675. CVE ID: CVE-2019-0673	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0673	A-MIC-OFFI- 040419/233
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0672, CVE-2019-0675. CVE ID: CVE-2019-0674	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0674	A-MIC-OFFI- 040419/234



Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0671, CVE-2019-0673, CVE-2019-0674. CVE ID: CVE-2019-0675	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad	A-MIC-OFFI- 040419/235
Edge					
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0590	https://port	A-MIC-EDGE- 040419/236
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting	https://port al.msrc.micr osoft.com/en	A-MIC-EDGE- 040419/237
CV Scoring Scal (CVSS)	0-1 1-		2-3 3-4 4-5 5-6 st Forgery; Dir. Trav Directory Tra	6-7 7-8	8-9 9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0591	-US/security- guidance/ad visory/CVE- 2019-0591	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0593	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0593	A-MIC-EDGE- 040419/238
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in	https://port al.msrc.micr osoft.com/en -US/security-	A-MIC-EDGE- 040419/239

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0605	guidance/ad visory/CVE- 2019-0605	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0607	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0607	A-MIC-EDGE- 040419/240
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad	A-MIC-EDGE- 040419/241

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019- 0590, CVE-2019-0591, CVE-2019-0593, CVE- 2019-0605, CVE-2019- 0607, CVE-2019-0640, CVE-2019-0642, CVE- 2019-0644, CVE-2019- 0651, CVE-2019-0652, CVE-2019-0655.	visory/CVE- 2019-0610	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0645, CVE-2019-0650.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0634	A-MIC-EDGE- 040419/242
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0642, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0640	A-MIC-EDGE- 040419/243

 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
			2019-0644, CVE-2019- 0651, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0640		
N/A	05-03-2019	4.3	A security feature bypass vulnerability exists in Microsoft Edge handles whitelisting, aka 'Microsoft Edge Security Feature Bypass Vulnerability'. CVE ID: CVE-2019-0641	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0641	A-MIC-EDGE- 040419/244
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0644, CVE-2019-0651, CVE-2019-0655.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0642	A-MIC-EDGE- 040419/245
			CVE ID : CVE-2019-0642		
N/A	05-03-2019	4.3	An information disclosure vulnerability exists in the way that Microsoft Edge handles cross-origin requests, aka 'Microsoft Edge Information Disclosure Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0643	A-MIC-EDGE- 040419/246

 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-2019-0643		
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0644	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0644	A-MIC-EDGE- 040419/247
N/A	05-03-2019	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0650. CVE ID: CVE-2019-0645	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0645	A-MIC-EDGE- 040419/248
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when Chakra improperly discloses the contents of its memory, which could provide an attacker with information to further compromise the user's	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0648	A-MIC-EDGE- 040419/249

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			computer or data.To exploit the vulnerability, an attacker must know the memory address of where the object was created.The update addresses the vulnerability by changing the way certain functions handle objects in memory, aka Scripting Engine Information Disclosure Vulnerability. This CVE ID is unique from CVE-2019- 0658. CVE ID: CVE-2019-0648		
N/A	05-03-2019	6.8	A vulnerability exists in Microsoft Chakra JIT server, aka 'Scripting Engine Elevation of Privileged Vulnerability'. CVE ID: CVE-2019-0649	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0649	A-MIC-EDGE- 040419/250
N/A	05-03-2019	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0634, CVE-2019-0645. CVE ID: CVE-2019-0650	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0650	A-MIC-EDGE- 040419/251
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad	A-MIC-EDGE- 040419/252

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0652, CVE-2019-0655. CVE ID: CVE-2019-0651	visory/CVE- 2019-0651	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0655. CVE ID: CVE-2019-0652	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0652	A-MIC-EDGE- 040419/253
N/A	05-03-2019	4.3	A spoofing vulnerability exists when Microsoft browsers improperly handles specific redirects, aka 'Microsoft Browser Spoofing Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-	A-MIC-EDGE- 040419/254

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0654	2019-0654	
N/A	05-03-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0590, CVE-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0651, CVE-2019-0652. CVE ID: CVE-2019-0655	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0655	A-MIC-EDGE- 040419/255
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0648. CVE ID: CVE-2019-0658	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0658	A-MIC-EDGE- 040419/256
Misp					
Misp					
N/A	01-03-2019	3.5	In MISP 2.4.102, an authenticated user can view sightings that they	N/A	A-MIS-MISP- 040419/257

 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
			should not be eligible for. Exploiting this requires access to the event that has received the sighting. The issue affects instances with restrictive sighting settings (event only / sighting reported only). CVE ID: CVE-2019-9482		
Mitel					
connect_onsit	le		A reflected Cross-site		
N/A	06-03-2019	4.3	scripting (XSS) vulnerability in ShoreTel Connect ONSITE before 19.49.1500.0 allows remote attackers to inject arbitrary web script or HTML via the brandUrl parameter. CVE ID: CVE-2019-9591	N/A	A-MIT- CONN- 040419/258
N/A	06-03-2019	4.3	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 19.45.1602.0 allows remote attackers to inject arbitrary web script or HTML via the url parameter. CVE ID: CVE-2019-9592	N/A	A-MIT- CONN- 040419/259
N/A	06-03-2019	4.3	A reflected Cross-site scripting (XSS) vulnerability in ShoreTel Connect ONSITE 18.82.2000.0 allows	N/A	A-MIT- CONN- 040419/260

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to inject arbitrary web script or HTML via the page parameter.		
			CVE ID : CVE-2019-9593		
my-netdata					
netdata					
N/A	15-03-2019	4.3	The Netdata web application through 1.13.0 allows remote attackers to inject their own malicious HTML code into an imported snapshot, aka HTML Injection. Successful exploitation will allow attacker-supplied HTML to run in the context of the affected browser, potentially allowing the attacker to steal authentication credentials or to control how the site is rendered to the user. CVE ID: CVE-2019-9834	N/A	A-MY NETD- 040419/261
nablarch_pro	ject				
nablarch					
N/A	12-03-2019	8.5	Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to conduct XML External Entity (XXE) attacks via unspecified vectors. CVE ID: CVE-2019-5918	N/A	A-NAB- NABL- 040419/262
N/A	12-03-2019	6.4	An incomplete cryptography of the data	N/A	A-NAB- NABL-

CV Scoring Scale	0-1	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
			store function by using hidden tag in Nablarch 5 (5, and 5u1 to 5u13) allows remote attackers to obtain information of the stored data, to register invalid value, or alter the value via unspecified vectors.		040419/263
			CVE ID : CVE-2019-5919		
Ncrafts					
Formcraft					
N/A	12-03-2019	6.8	Cross-site request forgery (CSRF) vulnerability in FormCraft 1.2.1 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page. CVE ID: CVE-2019-5920	N/A	A-NCR- FORM- 040419/264
njiandan-cms					
njiandan-cms	<u> </u>				
N/A	07-03-2019	6.8	njiandan-cms through 2013-05-23 has index.php/admin/user_ne w CSRF to add an administrator. CVE ID: CVE-2019-8437	N/A	A-NJI-NJIA- 040419/265
Openssl					
Openssl					
N/A	06-03-2019	5.8	ChaCha20-Poly1305 is an AEAD cipher, and requires a unique nonce input for every encryption operation. RFC 7539	https://ww w.openssl.or g/news/seca dv/2019030	A-OPE- OPEN- 040419/266
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	3-4 4-5 5-6	6-7 7-8	8-9 9-10
		_	st Forgery; Dir. Trav Directory Traves s Site Scripting; Sql- SQL Injection; N/		
			100		

Vulnerability Type(s)	Publish Da	te CVSS	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
			specifies th	at the no	once	6.txt			
			value (IV) s	hould be	e 96				
			bits (12 byt	es). Ope	nSSL				
			allows a va	riable no	nce				
			length and	front pa	ds the				
			nonce with	0 bytes	if it is				
			less than 12	bytes.					
			However it		•				
			allows a no						
			up to 16 bytes. In this case only the last 12 bytes are						
			_	significant and any additional leading bytes					
				_	ytes				
			are ignored						
			requiremer		_				
			cipher that						
			are unique.	_					
			encrypted ι	_	eused				
			nonce value						
			susceptible		us				
			confidentia	•					
			integrity at						
			application	_					
			default non	_					
			longer than then makes	-					
			leading byt	_					
			expecting the						
			be a new ur						
			then such a	•					
			could inady						
			encrypt me						
			reused non	•					
			the ignored		•				
			nonce are n	-					
			the integrit						
			this cipher.						
			application						
			the integrit						
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 Typ		_			-			nformatio	n; DoS-
	Denial of Serv	rice; XSS- Cros	s Site Scripting; 101	sql- SQL Ir	ijection; N	/A- Not A	oplicable.		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ignored leading bytes of a		
			long nonce may be further		
			affected. Any OpenSSL		
			internal use of this cipher,		
			including in SSL/TLS, is		
			safe because no such use		
			sets such a long nonce		
			value. However user		
			applications that use this		
			cipher directly and set a		
			non-default nonce length		
			to be longer than 12 bytes		
			may be vulnerable.		
			OpenSSL versions 1.1.1		
			and 1.1.0 are affected by		
			this issue. Due to the		
			limited scope of affected		
			deployments this has been		
			assessed as low severity		
			and therefore we are not		
			creating new releases at		
			this time. Fixed in OpenSSL		
			1.1.1c-dev (Affected 1.1.1-		
			1.1.1b). Fixed in OpenSSL		
			1.1.0k-dev (Affected 1.1.0-		
			1.1.0j).		
			CVE ID : CVE-2019-1543		
Openstack					
Neutron					
			An issue was discovered in		
			the iptables firewall		
			module in OpenStack		A-OPE-
N/A	12-03-2019	4	Neutron before 10.0.8,	N/A	NEUT-
11/11	12 00 2017	•	11.x before 11.0.7, 12.x	11/11	040419/267
			before 12.0.6, and 13.x		010117/207
			before 13.0.3. By setting a		
			destination port in a		

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID	Pa	itch	NCII	PC ID	
			security growith a protodoesn't suppoption (for every VRRP), an avery suser may bleapplication group rules from any pron the componity which it's application iptables security are as a composite componity or the componity and the componity and the componity are as a composite componity and the componity and the composite componity and the componity are as a composite componity and the componity and the componity and the composite componity and the componity and the composite componity and the composite composit						
openwsman_p	project								
openwsman									
N/A	14-03-2019	5	Openwsman to and inclu vulnerable t disclosure b working dir openwsman set to root d remote, una attacker can vulnerabilit specially cra request to o server. CVE ID : CV	illa.red m/sho	//bugz dhat.co ow_bug =CVE- 3816	A-OPE OPEN 04041			
N/A	14-03-2019	5	Openwsmar to and inclu vulnerable t in process_c when parsir crafted HTT	illa.red m/sho	//bugz dhat.co bw_bug =CVE- 3833	A-OPE OPEN- 04041			
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): 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	Descript	tion & CVE II	P	atch	NCIII	PC ID
			remote, una attacker car vulnerabilit malicious H cause denia	n exploit th ty by sendi ITTP reque	is ng st to			
			openwsmai		333			
Otrs								
Otrs								
N/A	13-03-2019	3.5	An issue was discovered in Open Ticket Request System (OTRS) 6.x before 6.0.17 and 7.x before 7.0.5. An attacker who is logged into OTRS as an admin user may manipulate the URL to cause execution of JavaScript in the context of OTRS. This is related to Kernel/Output/Template/ Document.pm. CVE ID: CVE-2019-9751		ore 7.0.5. ged the N/A n of ext of o		A-OTR OTRS- 04041	
N/A	13-03-2019	6.5	An issue was discovered in Open Ticket Request System (OTRS) 5.x before 5.0.34, 6.x before 6.0.16, and 7.x before 7.0.4. An attacker who is logged into OTRS as an agent or a customer user may upload a carefully crafted resource in order to cause execution of JavaScript in the context of OTRS. This is related to Content-type mishandling in Kernel/Modules/PictureU		ore 6, n into load N/A nuse t in his		A-OTR OTRS- 04041	
CV Scoring Sca	le 0-1 1	-2 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
			pload.pm.		
			CVE ID : CVE-2019-9752		
personal_vid	eo_collection_sc	ript_pr	oject		
personal_vid	eo_collection_sc	ript			
N/A	06-03-2019	3.5	PHP Scripts Mall Personal Video Collection Script 4.0.4 has Stored XSS via the "Update profile" feature. CVE ID: CVE-2019-9606	N/A	A-PER-PERS- 040419/272
PHP			CVEID I CVE ZOID 7000		
PHP					
N/A	08-03-2019	5	An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data. CVE ID: CVE-2019-9637	N/A	A-PHP-PHP- 040419/273
N/A	08-03-2019	7.5	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKE RNOTE because of	N/A	A-PHP-PHP- 040419/274

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			mishandling the maker_note->offset relationship to value_len. CVE ID: CVE-2019-9638		
N/A	08-03-2019	7.5	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKE RNOTE because of mishandling the data_len variable. CVE ID: CVE-2019-9639	N/A	A-PHP-PHP- 040419/275
N/A	08-03-2019	7.5	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn. CVE ID: CVE-2019-9640	N/A	A-PHP-PHP- 040419/276
N/A	08-03-2019	7.5	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF. CVE ID: CVE-2019-9641	N/A	A-PHP-PHP- 040419/277
N/A	11-03-2019	6.8	** DISPUTED ** An issue was discovered in PHP 7.x before 7.1.27 and 7.3.x before 7.3.3. phar_tar_writeheaders_int	N/A	A-PHP-PHP- 040419/278

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			in ext/phar/tar.c has a buffer overflow via a long link value. NOTE: The vendor indicates that the link value is used only when an archive contains a symlink, which currently cannot happen: "This issue allows theoretical compromise of security, but a practical attack is usually impossible." CVE ID: CVE-2019-9675		
phpmywind					
phpmywind					
N/A	07-03-2019	4.3	An issue was discovered in PHPMyWind 5.5. The username parameter of the /install/index.php page has a stored Crosssite Scripting (XSS) vulnerability, as demonstrated by admin/login.php. CVE ID: CVE-2019-7660	N/A	A-PHP- PHPM- 040419/279
N/A	07-03-2019	4.3	An issue was discovered in PHPMyWind 5.5. The method parameter of the data/api/oauth/connect.p hp page has a reflected Cross-site Scripting (XSS) vulnerability. CVE ID: CVE-2019-7661	N/A	A-PHP- PHPM- 040419/280
phpshe					
phpshe					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnorability Typo(s): CSPE Cross Site Poguest Forgary: Dir Tray Directory Trayersal: +Info Gain Information: Dos									a. Dos	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID								
N/A	07-03-2019	7.5	PHPSHE 1.7 allows module/index/cart.php pintuan_id SQL Injection to index.php. CVE ID: CVE-2019-9626	N/A	A-PHP-PHPS- 040419/281								
			An XXE issue was										
N/A	13-03-2019	5	discovered in PHPSHE 1.7, which can be used to read any file in the system or scan the internal network without authentication. This occurs because of the call to wechat_getxml in include/plugin/payment/wechat/notify_url.php. CVE ID: CVE-2019-9761	N/A	A-PHP-PHPS- 040419/282								
N/A	13-03-2019	7.5	A SQL Injection was discovered in PHPSHE 1.7 in include/plugin/payment/a lipay/pay.php with the parameter id. The vulnerability does not need any authentication. CVE ID: CVE-2019-9762	N/A	A-PHP-PHPS- 040419/283								
pivotal_software													
operations_manager													
N/A	07-03-2019	3.5	Pivotal Operations Manager, 2.1.x versions prior to 2.1.20, 2.2.x versions prior to 2.2.16, 2.3.x versions prior to 2.3.10, 2.4.x versions prior to 2.4.3, contains a reflected cross site scripting vulnerability. A	https://pivot al.io/security /cve-2019- 3776	A-PIV-OPER- 040419/284								
CV Scoring Scal (CVSS)	e 0-1 1-	2 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- SOL Injection: N/A- Not Applicable.													

Vulnerability Type(s)	Publish Da	ate	cvss	Descript	ion & CV	E ID	Pa	atch	NCII	PC ID							
				remote use convince ar Manager us with malici could execu JavaScript i browser.	o Operation of the Oper	ions eract ent ary											
				CVE ID : CV	E-2019	-3776											
spring_securi	spring_security_oauth Spring Security OAuth,																
N/A	07-03-201	9	6.4	versions 2.3 and 2.2 prior to 2.0 unsupporte could be su open redirecan leak an code. A mal attacker can request to tauthorization using the accode grant specify a more direct using the accode grant specify a more direct under the compart of the following the followin	B prior to 2.2. 2.1.4, and ad version sceptible ector attains authorizations us an eraft a he on endpouthorizatype, and anipulation serve eresource agent to ontrol outh the le on code. Ey exposes that me wing	o 2.3.5, 4, and ad 2.0 older as e to an ack that zation ser or oint tion d the act at at the act at the act at the act at a		//pivot security 2019-	A-PIV 04041	-SPRI- -9/285							
CV Scoring Scale (CVSS)	e 0-1	1-2	2	2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-1													
			_			_			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	Pa	itch	NCIII	PC ID
Server (e.g. @EnableAuthorizationSer ver) and uses the DefaultRedirectResolver in the AuthorizationEndpoint. This vulnerability does not expose applications that: Act in the role of an Authorization Server and uses a different RedirectResolver implementation other than DefaultRedirectResolver, act in the role of a Resource Server only (e.g. @EnableResourceServer), act in the role of a Client only (e.g. @EnableOAuthClient). CVE ID: CVE-2019-3778 pixar renderman A local privilege escalation vulnerability exists in the								
N/A	08-03-2019	7.2	•	exists in the ion of Pixar 2.3.0's Install tool. A user ess can use lity to privileges to ser would ess to the successful	N/A		A-PIX- 04041	REND- 9/286
CV Scoring Scal (CVSS)	0-1 1-			4-5 5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Si Denial of Service; X	-						n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
podofo_proje	ct	l			
podofo					
N/A	11-03-2019	7.5	PoDoFo 0.9.6 has a heap- based buffer overflow in PdfString::ConvertUTF16t oUTF8 in base/PdfString.cpp. CVE ID: CVE-2019-9687	N/A	A-POD- PODO- 040419/287
popojicms					
popojicms					
N/A	03-03-2019	6.8	An issue was discovered in PopojiCMS v2.0.1. It has CSRF via the poadmin/route.php?mod=us er&act=addnew URI, as demonstrated by adding a level=1 account, a similar issue to CVE-2018-18935. CVE ID: CVE-2019-9549	N/A	A-POP- POPO- 040419/288
Python					
Python					
N/A	08-03-2019	5	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit,	N/A	A-PYT- PYTH- 040419/289

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

quizandsurveymaster quiz_and_survey_master The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp- admin/admin.php?page= N/A A-QUI-QUIZ-	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n followed by an HTTP header or a Redis command. CVE ID : CVE-2019-9740 quizand_survey_master The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp- admin/admin.php?page= mlw_quiz_results quiz_id XSS. A-PYT- PYTH- 040419/290 A-QUI-QUIZ- 040419/291				attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.		
quiz_and_survey_master The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp- admin/admin.php?page= mlw_quiz_results quiz_id XSS. A-QUI-QUIZ- 040419/291	N/A	12-03-2019	4.3	urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.2. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n followed by an HTTP header or a Redis command.	N/A	
The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp- admin/admin.php?page= mlw_quiz_results quiz_id XSS. A-QUI-QUIZ- 040419/291	quizandsurve	ymaster				
N/A Master plugin 6.0.4 for WordPress allows wp-admin/admin.php?page=mlw_quiz_results quiz_id XSS. A-QUI-QUIZ-040419/291	quiz_and_sur	vey_master				
	N/A	05-03-2019	4.3	Master plugin 6.0.4 for WordPress allows wp-admin/admin.php?page=mlw_quiz_results quiz_id XSS.	N/A	A-QUI-QUIZ- 040419/291
rainbowpdf	rainbowpdf					
office_server_document_converter						

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	e CVSS	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
N/A	07-03-2019	7.5	A heap over vulnerability PowerPoint conversion Rainbow Pl Document (Pro R1 (7,0) While parsis Summary Pl stream, the getSummar function is checking the between size number of propertySe causing an write that lecorruption code executors (CVE ID : CVE ID :	N/A		A-RAI-0FFI- 040419/292			
rednao									
smart_forms									
N/A	12-03-2019	6.8	Cross-site request forgery (CSRF) vulnerability in Smart Forms 2.6.15 and earlier allows remote attackers to hijack the authentication of administrators via a specially crafted page. CVE ID: CVE-2019-5924			N/A		A-REI SMAR 04041	
RSA									
authenticatio	n_manager								
N/A	13-03-2019	4	RSA Auther Manager ve			N/A		A-RSA- AUTH-	
CV Scoring Scal (CVSS)	0-1		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; SqI- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			8.4 P1 contain an Insecure Credential Management Vulnerability. A malicious Operations Console administrator may be able to obtain the value of a domain password that another Operations Console administrator had set previously and use it for attacks. CVE ID: CVE-2019-3711		040419/294
archer_grc_pl	atform				
N/A	13-03-2019	2.1	RSA Archer versions, prior to 6.5 SP1, contain an information exposure vulnerability. Users' session information is logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed information to use it in further attacks. CVE ID: CVE-2019-3715	N/A	A-RSA- ARCH- 040419/295
N/A	13-03-2019	2.1	RSA Archer versions, prior to 6.5 SP2, contain an information exposure vulnerability. The database connection password may get logged in plain text in the RSA Archer log files. An authenticated malicious local user with access to the log files may obtain the exposed	N/A	A-RSA- ARCH- 040419/296

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			password to use it in further attacks. CVE ID: CVE-2019-3716		
Samba					
Samba					
N/A	06-03-2019	4	A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.	N/A	A-SAM- SAMB- 040419/297
			CVE ID : CVE-2019-3824		
SAP					
N/A 12-03-2019 5.5		SAP BusinessObjects Business Intelligence Platform (CMC Module), versions 4.10, 4.20 and 4.30, does not sufficiently validate an XML document accepted from an untrusted source. CVE ID: CVE-2019-0268	N/A	A-SAP-BUSI- 040419/298	
N/A	12-03-2019	3.5	SAP BusinessObjects Business Intelligence Platform (BI Workspace), versions 4.10 and 4.20, does not sufficiently encode user-controlled inputs, resulting in Cross-	N/A	A-SAP-BUSI- 040419/299

CV Scoring Scale	0.1	1.2	ງ ວ	2.4	4-5	Е 6	6.7	7.0	o 0	0.10
(CVSS)	0-1	1-2	2-5	5-4	4-5	3-0	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Pub	lish Date	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
					Scriptii ierabilit	ng (XSS) .y.					
				CVE	ID : CV	E-2019	-0269				
advanced_bu	siness	_applic	ation_pro	ogran	nming_	platforr	n_kerne	l		•	
N/A	12-03	3-2019	6.5	Plate neces authorized privers 7.21 7.22 7.21 KRN 7.21 7.22 8.04 7.49 8.04	NetWeaver and ABAP Platform fail to perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has been corrected in the following versions: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04. CVE ID: CVE-2019-0270 gramming_platform_krnl64nuc ABAP Server of SAP		N/A		A-SAP ADVA 04041		
advanced_bu	siness	_applic	ation_pro	ogran	nming_	platforr	n_krnl6	4nuc			
N/A	12-03	3-2019	6.5	Net' Plat neco chec auth resu priv corr				N/A		A-SAP ADVA 04041	
CV Scoring Scal (CVSS)		0-1		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty			s Site Reque e; XSS- Cros	_			-			normatio	ii; D05-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04. CVE ID: CVE-2019-0270		
advanced_bus	siness_applicati	on_pro	gramming_platform_krnl64	łuc	
N/A	12-03-2019	6.5	ABAP Server of SAP NetWeaver and ABAP Platform fail to perform necessary authorization checks for an authenticated user, resulting in escalation of privileges. This has been corrected in the following versions: KRNL32NUC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL32UC 7.21, 7.21EXT, 7.22, 7.22EXT, KRNL64NUC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04. CVE ID: CVE-2019-0270	N/A	A-SAP- ADVA- 040419/302
advanced_bus	siness_applicati	on_pro	gramming_platform_krnl32	2nuc	

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Viole and hills Tomo (a), CCRF, Cross Cite Dominat Forgow, Dir. Tray, Directory Tray, and June Coin Information, DoC										

Vulnerability Type(s)	Publish Date	cvss	Descrip	ion & CV	E ID	Pa	tch	NCII	PC ID
N/A	12-03-2019	6.5	ABAP Server NetWeaver Platform fancessary a checks for a authenticate resulting in privileges. Corrected in versions: K 7.21, 7.21E 7.22EXT, K 7.21EXT, 7. KRNL64NU 7.21EXT, 7. 7.49, 7.74, I 7.21, 7.21E 7.22EXT, 7. 8.04, KERN 7.49, 7.53, 2 8.04.	N/A		A-SAP ADVA- 04041			
advanced_bus	 siness_applicati	ion_pro	 gramming	platforr	n_krnl3	2uc			
N/A	12-03-2019	6.5	ABAP Server NetWeaver Platform far necessary as checks for a authenticate resulting in privileges. I corrected in versions: K 7.21, 7.21E 7.22EXT, K 7.21EXT, 7. KRNL64NU 7.21EXT, 7.	N/A		A-SAP ADVA- 04041			
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Ty	pe(s): CSRF- Cross Si Denial of Service;)	_		Sql- SQL Ir	-			normatio	II; DOS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			7.49, 7.74, KRNL64UC 7.21, 7.21EXT, 7.22, 7.22EXT, 7.49, 7.73, 7.74, 8.04, KERNEL 7.21, 7.45, 7.49, 7.53, 7.73, 7.74, 7.75, 8.04.	,	
advanced hu	siness annlicati	on pro	CVE ID : CVE-2019-0270 pgramming_platform		
N/A	12-03-2019	4	ABAP Server (used in NetWeaver and Suite/ERP) and ABAP Platform does not sufficiently validate an XML document accepted from an untrusted source, leading to an XML Externa Entity (XEE) vulnerability Fixed in Kernel 7.21 or 7.22, that is ABAP Server 7.00 to 7.31 and Kernel 7.45, 7.49 or 7.53, that is ABAP Server 7.40 to 7.52 or ABAP Platform. CVE ID: CVE-2019-0271	l N/A	A-SAP- ADVA- 040419/305
N/A	12-03-2019	4	ABAP Server (used in NetWeaver and Suite/ERP) and ABAP Platform does not sufficiently validate an XML document accepted from an untrusted source, leading to an XML Externa Entity (XEE) vulnerability. Fixed in Kernel 7.21 or 7.22, that is ABAP Server 7.00 to 7.31 and Kernel	1	A-SAP-SAP 040419/306
CV Scoring Scal	le 0-1 1-	-2 2	7.00 to 7.31 and Kerner	6-7 7-	8 8-9 9-10

Vulnerability Type(s)	Publish Dat	ce CVSS	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID		
			7.45, 7.49 o ABAP Serve or ABAP Pla	er 7.40 to							
			CVE ID : CV	CVE ID : CVE-2019-0271							
mobile_platfo	orm_sdk										
N/A	/A 12-03-2019 5			Platforr ttacker t itimate u sing a ser rashing o e service rvice). F 1 SP03 P 104, or lat	users rvice, or e (i.e. ixed in eL02, ter.	N/A			-MOBI- 9/307		
			CVE ID : CV	E-2019	-0274						
N/A	12-03-2019	3.5	SAML 1.1 SSO Demo Application in SAP NetWeaver Java Application Server (J2EE-APPS), versions 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40 and 7.50, does not sufficiently encode user-controlled inputs, which results in cross-site scripting (XSS) vulnerability. CVE ID: CVE-2019-0275			N/A		A-SAP NETW 04041			
banking_serv	rices_from_sa	ар									
N/A	12-03-2019	6.5	Banking services from SAP 9.0 (FSAPPL version 5) and SAP S/4HANA Financial Products Subledger (S4FPSL, version 1) performs an			N/A		A-SAP BANK 04041			
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10		
Vulnerability Ty		_	st Forgery; Dir.'s Site Scripting;		_				n; DoS-		

Vulnerability Type(s)	Publish Date	cvss		Descript	tion & CV	E ID	Pa	tch	NCII	PC ID
			che use in e	ck for an r, poten scalatio	authorized authentially results of priverse (E-2019)	ticated sulting rileges.				
s/4hana_fina	 ncial_products_	subled		E ID : CV	E-2019	-0276				
N/A	12-03-2019	6.5	Banking services from SAP 9.0 (FSAPPL version 5) and SAP S/4HANA Financial Products Subledger (S4FPSL, version 1) performs an inadequate authorization check for an authenticated user, potentially resulting in escalation of privileges. CVE ID: CVE-2019-0276			s an zation ticated sulting rileges.	N/A		A-SAP- 04041	
hana extende	ed_application_s	service		E ID : CV	E-2019	-02/6				
N/A	12-03-2019	5.5	SAP HANA extended application services, version 1, advanced does not sufficiently validate an XML document accepted from an authenticated developer with privileges to the SAP space (XML External Entity vulnerability). CVE ID: CVE-2019-0277			N/A		A-SAP- HANA- 04041	-	
schoolcms	<u>'</u>									
schoolcms	noolcms									
N/A	05-03-2019	6.5	SchoolCMS version 2.3.1 allows file upload via the theme upload feature at admin.php?m=admin&c=t				N/A		A-SCH-SCHO- 040419/312	
CV Scoring Scal	e 0-1 1-	2 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
			heme&a=upload by using the .zip extension along with the _Static substring, changing the Content-Typ to application/zip, and placing PHP code after the ZIP header. This ultimately allows execution of arbitrary PHP code in Public\Home\1_Static.php because of mishandling in the Application\Admin\Controller\ThemeController.class.php Upload() function.	y D	
scroon stroon	n project		CVE ID : CVE-2019-9572		
screen_strean					
N/A	15-03-2019	5	The Screen Stream application through 3.0.15 for Android allows remote attackers to cause a denial of service via many simultaneous /start-stop requests.		A-SCR-SCRE- 040419/313
			CVE ID : CVE-2019-9833		
sdcms sdcms					
N/A	10-03-2019	7.5	An issue was discovered in SDCMS V1.7. In the \app\admin\controller\tilde emecontroller.php file, the check_bad() function's filtering is not strict, resulting in PHP code execution. This occurs	1	A-SDC- SDCM- 040419/314
	9 01 1				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			because some dangerous PHP functions (such as "eval") are blocked but others (such as "system") are not, and because ".php" is blocked but ".PHP" is not blocked. CVE ID: CVE-2019-9651		
N/A	10-03-2019	6.8	There is a CSRF in SDCMS V1.7 via an m=admin&c=theme&a=edi t request. It allows PHP code injection by providing a filename in the file parameter, and providing file content in the t2 parameter. CVE ID: CVE-2019-9652	N/A	A-SDC- SDCM- 040419/315
sftnow					
sftnow					
N/A	11-03-2019	6.8	sftnow through 2018-12-29 allows index.php?g=Admin&m=U ser&a=add_post CSRF to add an admin account. CVE ID: CVE-2019-9688	N/A	A-SFT-SFTN- 040419/316
shanda			CVLID: CVL 2017 7000		
maplestory_o	nline				
N/A	12-03-2019	7.2	In Shanda MapleStory Online V160, the SdoKeyCrypt.sys driver allows privilege escalation to NT AUTHORITY\SYSTEM because of not validating	N/A	A-SHA- MAPL- 040419/317

Vulnerability Type(s)	Publish Dat	ce CVSS	Descrip	tion & CV	E ID	Pa	itch	NCII	PC ID
			the IOCtl 0x input value integer sign and a heap- underflow.	, leading iedness	to an error				
			CVE ID : CV	Æ-2019	-9729				
Solarwinds									
orion_platfor	m								
N/A	01-03-2019	7.5	SolarWinds before 201 allows priv through the service. CVE ID : CV	8.4 Hotfi ilege esc e Rabbitl	x 2 alation MQ	ort.solds.com ess_Ce rion_F m/Ori ument Additi esoure	on_Doc tation/ onal_R ces/Ori atform_		-ORIO- 9/318
spdk									
storage_perfo	ormance_dev	elopment	_kit						
N/A	01-03-2019	5	In Storage In Developme before 19.0 whost client machine) construct a descriptor would resudenial of sets SPDK whost the whost taproperly dechains. CVE ID: CV	b.com spdk/	//githu /spdk/ release 'v19.01		-STOR- 9/319		
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty		_	st Forgery; Dir. s Site Scripting;		-			nformatio	n; DoS-

Vulnerability Type(s)	Publish Da	te CVSS	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID	
stackstorm										
stackstorm										
N/A	08-03-201	9 4.3	In st2web i Web UI bef 2.10.x befo possible to CORS prote mechanism origin valu leading to 2 CVE ID : CV	fore 2.9.3 re 2.10.3 bypass tection via a "ne, potent	and , it is he ull" ially	N/A			-STAC- 9/320	
theolivetree										
ftp_server										
_			The Olive 7	ree FTP	Server					
N/A	06-03-201	9 5	The Olive Tree FTP Server (aka com.theolivetree.ftpserver) application through 1.32 for Android allows remote attackers to cause a denial of service via a client that makes many connection attempts and drops certain packets. CVE ID: CVE-2019-9600			N/A		A-THE-FTP 040419/321		
thinkst										
canarytokens										
N/A	14-03-201	9 5	Thinkst Canarytokens through 2019-03-01 relies on limited variation in size, metadata, and timestamp, which makes it easier for attackers to estimate whether a Word document contains a token. CVE ID: CVE-2019-9768			N/A			-CANA- .9/322	
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 Ty			st Forgery; Dir. s Site Scripting;		_			nformatio	n; DoS-	

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CV	E ID	Pa	atch	NCII	PC ID
Tibco									
jasperreports	s_server								
N/A	07-03-2019	4	vulnerability that may allow a malicious authenticated user to copy text files from the host operating system. Affected releases are TIBCO Software Inc.'s TIBCO JasperReports Server: versions up to and including 6.3.4; 6.4.0;		https://ww w.tibco.com/ support/advi sories/2019/ 03/tibco- security- advisory- march-6- 2019-tibco- jasperreport s-server- 2018-8986		A-TIB- 04041	-JASP- 9/323	
tinycc									
tinycc									
N/A	13-03-2019	4.3	An issue was discovered in Tiny C Compiler (aka TinyCC or TCC) 0.9.27. Compiling a crafted source file leads to an 1 byte out of bounds write in the end_macro function in tccpp.c. CVE ID: CVE-2019-9754		N/A			-TINY- 9/324	
CV Scoring Scal (CVSS)	e 0-1 1- pe(s): CSRF- Cross Sit		2-3 3-4 st Forgery: Dir.	4-5 Trav Dire	5-6	6-7 ersal: +Ir	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
tinysvcmdns	project	_				
tinysvcmdns						
N/A	13-03-2019	5	In tinysvcmdns through 2018-01-16, a maliciously crafted mDNS (Multicast DNS) packet triggers an infinite loop while parsing an mDNS query. When mDNS compressed labels point to each other, the function uncompress_nlabel goes into an infinite loop trying to analyze the packet with an mDNS query. As a result, the mDNS server hangs after receiving the malicious mDNS packet. NOTE: the product's web site states "This project is un-maintained, and has been since 2013 There are known vulnerabilities You are advised to NOT use this library for any new projects / products." CVE ID: CVE-2019-9747	N/A	A-TIN-TINY- 040419/325	
			In tinysvcmdns through 2018-01-16, an mDNS server processing a crafted			
N/A	13-03-2019	9.4	packet can perform arbitrary data read operations up to 16383 bytes from the start of the buffer. This can lead to a segmentation fault in uncompress_nlabel in	N/A	A-TIN-TINY- 040419/326	

mdns.c and a crash of the server (depending on the memory protection of the CPU and the operating system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
memory protection of the CPU and the operating system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
CPU and the operating system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
system), or disclosure of memory content via error messages or a server response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
memory content via error messages or a server response. NOTE: the product's web site states "This project is un- maintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
messages or a server response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
response. NOTE: the product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
product's web site states "This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
"This project is unmaintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
maintained, and has been since 2013 There are known vulnerabilities You are advised to NOT	
since 2013 There are known vulnerabilities You are advised to NOT	
known vulnerabilities You are advised to NOT	
You are advised to NOT	
	i e
use this library for any	
new projects / products."	
CVE ID : CVE-2019-9748	
treasuredata	
fluent_bit	
An issue was discovered in	
the MQTT input plugin in	
Fluent Bit through 1.0.4.	
When this plugin acts as an MQTT broker (server), it	
mishandles incoming	
network messages. After	
processing a crafted	
nacket, the plugin's	A-TRE-FLUE-
N/A 13-03-2019 5 packet, the plught 3 N/A mqtt_packet_drop function	040419/327
(in	010113/027
/plugins/in_mqtt/mqtt_pr	
ot.c) executes the	
memmove() function with	
a negative size parameter.	
That leads to a crash of the	
whole Fluent Bit server via	
a SIGSEGV signal.	
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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS-Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9749		
twinkletoesso	oftware			<u> </u>	
booked					
N/A	05-03-2019 7.5 R		phpscheduleit Booked Scheduler 2.7.5 allows arbitrary file upload via the Favicon field, leading to execution of arbitrary Web/custom-favicon.php PHP code, because Presenters/Admin/Manag eThemePresenter.php does not ensure an image file extension. CVE ID: CVE-2019-9581	N/A	A-TWI- BOOK- 040419/328
Vanillaforum	s				
vanilla_forum	15				
N/A	01-03-2019	3.5	Multiple stored XSS in Vanilla Forums before 2.5 allow remote attackers to inject arbitrary JavaScript code into any message on forum. CVE ID: CVE-2019-8279	N/A	A-VAN-VANI- 040419/329
wdoyo					
doyocms					
N/A	03-03-2019	3.5	An issue was discovered in DOYO (aka doyocms) 2.3 through 2015-05-06. It has admin.php XSS. CVE ID: CVE-2019-9551	N/A	A-WDO- DOYO- 040419/330
Webkitgtk					
Webkitgtk+					

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CV33)										

Vulnerability Type(s)	Publish Date	cvss	Description & CV	E ID	Patch		NCIII	PC ID
N/A	05-03-2019	6.8	A memory corruption issue was addressed improved memory handling. This issue fixed in iOS 12.1.3, to 12.1.2, Safari 12.0.3 iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Proceeding the content may lead to arbitrary code executive code executive.	is vOS, resisting web	https://s ort.apple m/HT20 ⁰ 1	.co	A-WEE WEBK 04041	-
Webmin	<u> </u>							
Webmin								
N/A	07-03-2019	6.8	Webmin 1.900 allow remote attackers to execute arbitrary colleveraging the "Java manager" and "Uplo Download" privilegoupload a crafted .cgi via the /updown/upload.cg	ode by file oad and es to i file	N/A		A-WEE WEBM 04041	[-
webmproject								
libwebm								
N/A	13-03-2019	5	In libwebm before 2019- 03-08, a NULL pointer dereference caused by the functions OutputCluster and OutputTracks in webm_info.cc will trigger an abort, which allows a DoS attack, a similar issue to CVE-2018-19212.		N/A		A-WEE LIBW- 04041	
CV Scoring Scal	e 0-1 1-	2 2	3-4 4-5	5-6	6-7	7-8	8-9	9-10
		-	st Forgery; Dir. Trav Dire	-			formatio	n; DoS-
	Demarui Service; A	.33- CrOS	Site Scripting; Sql- SQL In 130	jection; N/A	- MOL APPII	capie.		

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	tion & CV	E ID	Pa	atch	NCI	IPC ID
					CVI	E ID : CV	E-2019	-9746				
Wordpress											•	
Wordpress												
N/A	14	-03-201	9	6.8	doe con to F by u in a Thi pro and Opt is p lead according according to the control of the contr	s not proment contents of the		ilter eading ecution users ration. e CSRF ndled, Engine lements ectly, XSS rative s o .php to wp-	N/A		A-W0 W0RI 04043	
Yzmcms					CVI	E ID : CV	E-2019	-9787				
Yzmcms												
N/A	05	-03-201	9	3.5	Yzn via the adn ve.l site	nCMS 5 the bott nin/syst ntml URI _code pa	as discov 2.0. It ha om text em_mar I, related aramete TE-2019	as XSS field to nage/sa I to the r.	N/A		A-YZM YZMC 0404	
N/A		-03-201	9	3.5	Yzn	nCMS 5.	exists in 2 via the gory/ed	!	N/A		A-YZM	
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				_				ectory Trav njection; N				on; DoS-

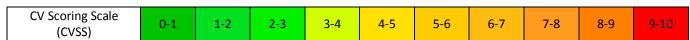
Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			"catname" parameter.		040419/336
			CVE ID : CVE-2019-9660		
N/A	11-03-2019	3.5	Stored XSS exists in YzmCMS 5.2 via the admin/system_manage/us er_config_edit.html "value" parameter,	N/A	A-YZM- YZMC- 040419/337
			CVE ID : CVE-2019-9661		
			OS		
Apple					
Tvos					
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved lock state checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes. CVE ID: CVE-2019-6205	N/A	O-APP-TVOS- 040419/338
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS- 040419/339

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
			CVE ID : CVE-2019-6212		
N/A	05-03-2019	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	N/A	O-APP-TVOS- 040419/340
			CVE ID : CVE-2019-6215		
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution.	https://supp ort.apple.co m/HT20945	O-APP-TVOS- 040419/341
			CVE ID : CVE-2019-6216		
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to	https://supp ort.apple.co m/HT20945	O-APP-TVOS- 040419/342

Vulnerability Type(s)	Publis	sh Dat	e C	CVSS		Descrip	tion & C\	Æ ID	Pa	itch	NCI	IPC ID
						•	ode exec 7 E-201 9					
N/A	05-03-	-2019	Ç	9.3	issu imp This 12.3 10.1 mal be a arbi	te was a proved it is issue it 1.3, mad 14.3, tv icious a lible to e itrary co vileges.	s fixed i OS Moja OS 12.1. pplicati xecute	d with idation. n iOS ove 2. A on may	N/A			P-TVOS- 19/343
N/A	05-03-	-2019	6	5.8	issu imp issu mad tvO app elev	te was a proved was in fixed cOS Moj S 12.1.2 lication wate priv	Ü	d with n. This 12.1.3, 4.3, cious able to	N/A			P-TVOS- 19/344
N/A	05-03-			5.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6226		ort.ap	//supp ple.co 20945		P-TVOS- 19/345		
N/A CV Scoring Scale	05-03-	2019	6	5.8	A m	emory	corrupt	on	https:	//supp	O-API	P-TVOS-
(CVSS) Vulnerability Ty	U	-1 RF- Cros	1-2 ss Site F		-3 st Forg	3-4 gery; Dir.	4-5 Trav Dir	5-6 ectory Trav	6-7 versal; +In	7-8 Ifo- Gain I	8-9 nformation	9-10 on: DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6227	ort.apple.co m/HT20945 1	040419/346
N/A	05-03-2019	4.3	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to universal cross site scripting. CVE ID: CVE-2019-6229	https://supp ort.apple.co m/HT20945	O-APP-TVOS- 040419/347
N/A	05-03-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3,macOS Mojave 10.14.3,tvOS 12.1.2,watchOS 5.1.3. A malicious application may be able to break out of its sandbox. CVE ID: CVE-2019-6230	https://supp ort.apple.co m/HT20944 8	O-APP-TVOS- 040419/348



Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	4.3	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to read restricted memory. CVE ID: CVE-2019-6231	https://supp ort.apple.co m/HT20944 8	O-APP-TVOS- 040419/349
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6233	https://supp ort.apple.co m/HT20945	O-APP-TVOS- 040419/350
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6234	https://supp ort.apple.co m/HT20945	O-APP-TVOS- 040419/351

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Watchos					
N/A	05-03-2019	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. A malicious application may be able to elevate privileges. CVE ID: CVE-2019-6202	https://supp ort.apple.co m/HT20944 8	O-APP- WATC- 040419/352
N/A	05-03-2019	4.3	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to determine kernel memory layout. CVE ID: CVE-2019-6209	N/A	O-APP- WATC- 040419/353
N/A	05-03-2019	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID: CVE-2019-6210	https://supp ort.apple.co m/HT20944 8	O-APP- WATC- 040419/354
N/A	05-03-2019	9.3	A buffer overflow was addressed with improved	N/A	O-APP- WATC-

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID	Pa	tch	NCII	PC ID
			macOS Moja tvOS 12.1.2, An applicati to execute a with kernel	d in iOS 12.1.3, ave 10.14.3, watchOS 5.1.3. on may be able rbitrary code			04041	9/355
N/A	05-03-2019	6.8	addressed v memory had issue is fixed macOS Moja tvOS 12.1.2, A malicious may be able its sandbox.	d in iOS 12.1.3, ave 10.14.3, watchOS 5.1.3. application to break out of	N/A		O-APP WATC 04041	
N/A	05-03-2019	6.8	addressed v memory had issue is fixed tvOS 12.1.2, iTunes 12.9 Windows, iO Windows 7. maliciously content may arbitrary co	d in iOS 12.1.3, Safari 12.0.3, .3 for Cloud for 10. Processing crafted web	N/A		O-APP WATC 04041	
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3		ort.ap	//supp ple.co 20945	O-APP WATC 04041	
CV Scoring Scal	e 0-1 1	-2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID	Pa	tch	NCII	IPC ID
			Windows 7 maliciously content ma arbitrary co	vs, iCloud for .10. Processing crafted web y lead to ode execution.				
N/A	05-03-2019	6.8	Multiple me corruption addressed was memory had issue is fixe tvOS 12.1.2 Safari 12.0.5 for Windows 7 maliciously content magarbitrary	emory issues were with improved ndling. This d in iOS 12.1.3, , watchOS 5.1.3, 3, iTunes 12.9.3 vs, iCloud for .10. Processing crafted web	ort.ap	//supp ple.co 20945	0-APF WATO 04041	
N/A	05-03-2019	5	A denial of swas addres improved vissue is fixe macOS MojawatchOS 5. a malicious message madenial of se	service issue sed with alidation. This d in iOS 12.1.3, ave 10.14.3, 1.3. Processing ly crafted ay lead to a rvice.	ort.ap	//supp ple.co 20944	O-APF WATO 04041	
N/A	05-03-2019	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A remote attacker may be		N/A		O-APF WATO 04041	
CV Scoring Scal	e 0-1 1	-2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CVE ID	Pa	itch	NCII	PC ID
				ate a FaceTime arbitrary code				
			CVE ID : CV	E-2019-6224				
N/A	05-03-2019	6.8	addressed v memory ha issue is fixe tvOS 12.1.2 Safari 12.0. for Window Windows 7 maliciously content ma	issues were with improved ndling. This d in iOS 12.1.3, watchOS 5.1.3, iTunes 12.9.3 vs, iCloud for 10. Processing crafted web	https:/ ort.ap m/HT	//supp ple.co 20945	O-APF WATO 04041	
			CVE ID : CV	E-2019-6226				
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6227		ort.ap	https://supp ort.apple.co m/HT20945 1		9- :- :9/363
N/A	05-03-2019	6.8	A memory issue was a improved n handling. T fixed in iOS Mojave 10.2	ort.ap	//supp ple.co 20944	O-APF WATO 04041		
CV Scoring Scal	e 0 -1 1	-2 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	
			malicious application may be able to break out of its sandbox. CVE ID: CVE-2019-6230						
N/A	05-03-2019	4.3	macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3.			https://supp ort.apple.co m/HT20944 8		O-APP- WATC- 040419/365	
watch_os			avz ib i d	- E = 017	0201				
N/A	04-03-2019	7.5	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, iTunes 12.9.3 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. CVE ID: CVE-2019-6235		https://supp ort.apple.co m/HT20945 0		O-APP- WATC- 040419/366		
iphone_os									
N/A	05-03-2019	5.8	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3. An attacker in a privileged network position may be able to execute arbitrary		https://supp ort.apple.co m/HT20944 6		O-APP-IPHO- 040419/367		
CV Scoring Scale (CVSS)	e 0-1	1-2 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			Pa	atch	NCIIPC ID		
			code. CVE ID : CV							
N/A	05-03-2019	6.8	An out-of-baddressed whounds che issue is fixed macOS Moj watchOS 5. application elevate privilege CVE ID : CV	ort.ap	//supp ple.co '20944	O-APP-IPHO- 040419/368				
N/A	05-03-2019	6.8	A memory issue was a improved lead the checking. The fixed in iOS Mojave 10.12.1.2. A mapplication unexpected memory shaprocesses. CVE ID: CV	N/A		O-APP-IPHO- 040419/369				
N/A	04-03-2019	5	An issue existed with autofill resuming after it was canceled. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.3. Password autofill may fill in passwords after they were manually cleared. CVE ID: CVE-2019-6206			ort.ap	//supp ple.co 20944	_	P-IPHO- 19/370	
N/A	05-03-2019	4.3	A memory initialization issue was addressed with			N/A		0-APP-IPH0- 040419/371		
CV Scoring Scal (CVSS)	e 0-1 pe(s): CSRF- Cross		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	
vunierability Ty	Denial of Service	_		Sql- SQL Ir	_			normatic	ni, DU3-	

Vulnerability Type(s)	Publish Date	cvss	Descript	Patch		NCIIPC ID			
			improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes. CVE ID: CVE-2019-6208						
N/A	05-03-2019	4.3	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to determine kernel memory layout. CVE ID: CVE-2019-6209		N/A		O-APP-IPHO- 040419/372		
N/A	05-03-2019	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID: CVE-2019-6210		https://supp ort.apple.co m/HT20944 8		O-APP-IPHO- 040419/373		
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved state			https://supp ort.apple.co m/HT20944		O-APP-IPHO- 040419/374	
CV Scoring Scal (CVSS)	e 0-1 1-	2 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				Pa	tch	NCIIPC ID		
			fixed in iOS Mojave 10.2 maliciously content ma arbitrary co	ode execution.	6				
N/A	05-03-2019	6.8	Multiple me corruption addressed was memory hard issue is fixed two S 12.1.2 iTunes 12.9 Windows, it windows 7 maliciously content may arbitrary content to the content may arbitrary content may arbi	N/A		O-APP-IPHO- 040419/375			
N/A	05-03-2019	9.3	A buffer over addressed with kernel	N/A			9-IPHO- 9/376		
N/A	05-03-2019	6.8	A type conf addressed v memory ha issue is fixe macOS Moj tvOS 12.1.2 A malicious	N/A			9-IPHO- 9/377		
CV Scoring Scal	e 0-1 1	-2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10	

Vulnerability Type(s)	Publish Date	cvss	Descripti	on & CVE	ID	Pa	tch	NCII	PC ID
			may be able its sandbox.	to break	out of				
			CVE ID : CV	E-2019-6	6214				
N/A	05-03-2019	6.8	A type confu addressed w memory har issue is fixed tvOS 12.1.2, iTunes 12.9. Windows, iO Windows 7.3 maliciously content may arbitrary con	vith improdling. The safari 12 safari 12 safari 12 safari 10 do no constitution of the safari to de execurated was de execurated to de execura	oved nis 2.1.3, 2.0.3, essing veb tion.	N/A		_	9-IPHO- 9/378
			CVE ID : CV	E-2019-6	5215				
N/A	05-03-2019	6.8	Multiple me corruption is addressed with memory hard issue is fixed tvOS 12.1.2, Safari 12.0.3 for Windows 7.3 maliciously content may arbitrary coccurrent CVE ID : CVI	ssues we with improding. The ding. The watchOS, iTunes iCloud 10. Proceed we lead to de execur	oved nis 2.1.3, 5.1.3, 12.9.3 for essing veb	https:/ ort.apj m/HT 1			°-IPHO- 9/379
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, watchOS 5.1.3, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing			https://supp ort.apple.co m/HT20945			9-IPHO- 9/380
CV Scoring Scal	le 0-1 1-	-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CVSS) Vulnerability Tv	/pe(s): CSRF- Cross Si								

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID	
			maliciously content ma arbitrary c	ay lead to ode exec	ution.					
N/A	05-03-2019	9.3	A memory issue was a improved in This issue 12.1.3, made 10.14.3, two malicious abe able to carbitrary coprivileges. CVE ID:	nddresse input val is fixed in cOS Moja OS 12.1.2 application execute ode with	d with idation. n iOS ve 2. A on may kernel	N/A			9-IPHO- 9/381	
N/A	05-03-2019	5	A denial of was addressing improved vissue is fixed macOS MowatchOS 5 a malicious message madenial of second CVE ID : CV	ssed with validation ed in iOS jave 10.1 .1.3. Prod sly crafte lay lead t ervice.	n. This 12.1.3, 4.3, cessing d o a	ort.ap	//supp ple.co 20944		9-IPHO- 9/382	
N/A	05-03-2019	6.8	An out-of-laddressed bounds che issue is fixed macOS Mo iTunes 12. Windows, application elevate pri CVE ID : CV	with impecking. Ted in iOS jave 10.1 9.3 for A malicida may be vileges.	oroved his 12.1.3, 4.3, ous able to	ort.ap m/HT 0	20945	04041	9-IPHO- 9/383	
N/A CV Scoring Scal	05-03-2019 e		A logic issu	e existed	l in the	https:/	//supp 7-8	0-APP 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.									

Type(s)	Pı	ublish Da	ite	CVSS		Descript	tion & CV	E ID	Pa	atch	NCI	IPC ID
					Face was imp man fixed Moja Sup initi Face to ca	addres roved stagement of a contract of a co	alls. The sed with tate nt. This i 12.1.4, i	ssue is macOS te. The oe able nt to	_	ple.co '20952	04041	19/384
N/A	05-	03-201	9	6.8	was imp hand fixed Moja 12.1 rem able call exec	addres roved node and in iOS ave 10	erflow is sed with nemory his issue 12.1.3, tvO chOS 5.1 acker ma ate a Fac g arbitran	e is macOS SS3. A y be ceTime cy code	N/A			P-IPHO- 19/385
N/A	05-	03-201	9	6.8	issu imp issu mac tvOS appl elev	e was a roved ve is fixe OS Moj S 12.1.2 dication ate priv	ddressed alidation d in iOS ave 10.1 . A malid may be vileges.	d with n. This 12.1.3, 4.3, cious able to	N/A			P-IPHO- 19/386
N/A	05-	5-03-2019 6.8 Multiple memory corruption issues were addressed with improved				ort.ap	//supp ple.co 20945		P-IPHO- 19/387			
CV Scoring Scale (CVSS) Vulnerability Typ		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	Descript	ion & CVE	ID	Pa	tch	NCII	PC ID
			memory ha issue is fixe tvOS 12.1.2 Safari 12.0.3 for Window Windows 7 maliciously content may arbitrary co	d in iOS 1, watchOS 3, iTunes 7s, iCloud 10. Proce crafted v y lead to	2.1.3, 5.1.3, 12.9.3 for essing yeb tion.	1			
N/A	05-03-2019	6.8	A memory of issue was actimproved in handling. The fixed in iOS 12.1.2, water Safari 12.0.3 for Windows 7 maliciously content may arbitrary co	ddressed nemory his issue i 12.1.3, tv chOS 5.1.3 3, iTunes vs, iCloud .10. Proce crafted w y lead to ode execu	with s OS 3, 12.9.3 for essing yeb tion.	https:/ ort.apj m/HT 1			P-IPHO- 9/388
N/A	05-03-2019	4.3	A cross-site existed in Sa was address improved U This issue is 12.1.3, Safai Processing crafted web lead to a croscripting at CVE ID : CV	afari. This sed with IRL validates fixed in ri 12.0.3. malicious ocontent toss site tack.	s issue ation. iOS aly may	https:/ ort.apj m/HT 9			P-IPHO- .9/389
N/A	05-03-2019	4.3	A logic issue was addressed with improved validation. This issue is			https:/ ort.apj m/HT			P-IPHO- .9/390
CV Scoring Scal (CVSS)	e 0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE ID	Pa	atch	NCII	PC ID
			12.1.2, Safa iTunes 12.9 Windows, it Windows 7 maliciously content may universal cr scripting.	0.3 for Cloud for 0.10. Processing 0. crafted web 19 lead to	1			
N/A	05-03-2019	6.8	issue was ad improved m handling. The fixed in iOS Mojave 10.1 12.1.2, watcomalicious at the able to be sandbox.	his issue is 12.1.3,macOS	ort.ap m/HT	//supp ple.co '20944		9-IPHO- 9/391
N/A	05-03-2019	4.3	An out-of-b addressed v bounds che issue is fixe macOS Moja tvOS 12.1.2 A malicious may be able restricted n	ounds read wa with improved cking. This d in iOS 12.1.3, ave 10.14.3, watchOS 5.1.3 application e to read	https: ort.ap	//supp ple.co '20944		9-IPHO- 9/392
N/A	05-03-2019	6.8	improved n handling. T	ddressed with nemory his issue is 12.1.3, tvOS	ort.ap	//supp ple.co '20945		P-IPHO- 9/393
CV Scoring Scal	e 0-1	1-2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
					Win Win mal con arb	nes 12.9 ndows, indows 7 liciously tent mag itrary co	Cloud fo .10. Prod crafted y lead to ode exec	cessing web ution.				
N/A	05	-03-201	9	6.8	issu imp han fixe 12. iTu Win Win con arb	nemory of the was a proved in adding. The din iOS 1.2, Safandows, indows 7 diciously attent magistrary contrary	ddressed nemory his issue 12.1.3, to ri 12.0.3 .3 for Cloud fo .10. Prod crafted y lead to ode exec	e is tvOS r cessing web oution.	ort.ap	//supp ple.co 20945		9-IPHO- 9/394
N/A	04	-03-201	9	7.5	issu imp issu mad tvO iTu Win pro circ	nemory of the was a proved vote is fixed to the cost of the cost o	ddressed alidation d in iOS ave 10.1 , watchO .3 for a sandbo y be able sandbo	d with n. This 12.1.3, 4.3, 0S 5.1.3, exed e to x	ort.ap	//supp ple.co 20945	_	9-IPHO- 9/395
mac_os_x												
N/A	N/A 05-03-2019 5.8					An out-of-bounds read was addressed with improved input validation. This issue			ort.ap	//supp ple.co 20944	O-APP MAC 04041	
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; Dos- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable. 150											

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			is fixed in iOS 12.1.3, macOS Mojave 10.14.3. An attacker in a privileged network position may be able to execute arbitrary code.	6		
			CVE ID : CVE-2019-6200			
N/A	05-03-2019	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, watchOS 5.1.3. A malicious application may be able to elevate privileges.	https://supp ort.apple.co	O-APP- MAC 040419/397	
			CVE ID : CVE-2019-6202			
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved lock state checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in memory shared between processes. CVE ID: CVE-2019-6205	N/A	0-APP- MAC 040419/398	
N/A	05-03-2019	4.3	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may cause unexpected changes in	N/A	O-APP- MAC 040419/399	
CV Scoring Scale	e 0-1 1·	-2 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
			memory shared between processes. CVE ID: CVE-2019-6208		
N/A	05-03-2019	4.3	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to determine kernel memory layout.	N/A	O-APP- MAC 040419/400
			CVE ID : CVE-2019-6209		
N/A	05-03-2019	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to execute arbitrary code with kernel privileges.	https://supp ort.apple.co m/HT20944 8	O-APP- MAC 040419/401
			CVE ID : CVE-2019-6210		
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3. Processing maliciously crafted web content may lead to arbitrary code execution.	https://supp ort.apple.co m/HT20944 6	O-APP- MAC 040419/402

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6211		
N/A	05-03-2019	9.3	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. An application may be able to execute arbitrary code with kernel privileges. CVE ID: CVE-2019-6213	N/A	O-APP- MAC 040419/403
N/A	05-03-2019	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to break out of its sandbox. CVE ID: CVE-2019-6214	N/A	O-APP- MAC 040419/404
N/A	05-03-2019	9.3	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID: CVE-2019-6218	N/A	O-APP- MAC 040419/405
N/A	05-03-2019	5	A denial of service issue was addressed with improved validation. This issue is fixed in iOS 12.1.3,	https://supp ort.apple.co m/HT20944 8	O-APP- MAC 040419/406

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			macOS Mojave 10.14.3, watchOS 5.1.3. Processing a maliciously crafted message may lead to a denial of service. CVE ID: CVE-2019-6219		
N/A	05-03-2019	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Mojave 10.14.3. An application may be able to read restricted memory. CVE ID: CVE-2019-6220	https://supp ort.apple.co m/HT20944 6	O-APP- MAC 040419/407
N/A	05-03-2019	6.8	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, iTunes 12.9.3 for Windows. A malicious application may be able to elevate privileges. CVE ID: CVE-2019-6221	https://supp ort.apple.co m/HT20945 0	O-APP- MAC 040419/408
N/A	05-03-2019	5	A logic issue existed in the handling of Group FaceTime calls. The issue was addressed with improved state management. This issue is fixed in iOS 12.1.4, macOS Mojave 10.14.3 Supplemental Update. The initiator of a Group FaceTime call may be able to cause the recipient to	https://supp ort.apple.co m/HT20952	O-APP- MAC 040419/409

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			answer. CVE ID : CVE-2019-6223		
N/A	05-03-2019	6.8	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A remote attacker may be able to initiate a FaceTime call causing arbitrary code execution. CVE ID: CVE-2019-6224	N/A	O-APP- MAC 040419/410
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2. A malicious application may be able to elevate privileges.	N/A	O-APP- MAC 040419/411
N/A	05-03-2019	6.8	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3,macOS Mojave 10.14.3,tvOS 12.1.2,watchOS 5.1.3. A malicious application may be able to break out of its sandbox. CVE ID: CVE-2019-6230	https://supp ort.apple.co m/HT20944 8	O-APP- MAC 040419/412
N/A	05-03-2019	4.3	An out-of-bounds read was addressed with improved	https://supp ort.apple.co	O-APP- MAC

Windows. A sandboxed process may be able to circumvent sandbox restrictions. CVE ID : CVE-2019-6235 CVE ID : CVE-2019-6235 CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser. CVE ID : CVE-2019-5616	Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID				
issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, iTunes 12.9.3 for Windows. A sandboxed process may be able to circumvent sandbox restrictions. CVE ID: CVE-2019-6235 CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser. CVE ID: CVE-2019-5616				issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3. A malicious application may be able to read restricted memory.	· ·	040419/413				
CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's webbrowser. CVE ID: CVE-2019-5616	N/A	04-03-2019	7.5	issue was addressed with improved validation. This issue is fixed in iOS 12.1.3, macOS Mojave 10.14.3, tvOS 12.1.2, watchOS 5.1.3, iTunes 12.9.3 for Windows. A sandboxed process may be able to circumvent sandbox restrictions.	ort.apple.co m/HT20945	MAC				
CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's webbrowser. CVE ID: CVE-2019-5616	broadcastbox	xes								
hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's webbrowser. CVE ID: CVE-2019-5616	scion-8_firmv	ware								
Canonical	N/A	15-03-2019	5	hardware device used for managing electrical devices, ships with a webbased front-end controller and implements an authentication mechanism in JavaScript that is run in the context of a user's web browser.	N/A					
	Canonical									
ubuntu_linux	ubuntu_linux	ubuntu_linux								

CV Scoring Scale (CVSS)

0-1

1-2

2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

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

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
N/A	06-03-2019	4	A flaw was way an LDA expression shared LDA process of a in samba be 4.10. An autuser, having permission server, coul to cause detection to cause detection.	AP search could cr P serven I samba efore ver thentica g read s on the d use th	ash the AD DC rsion ted LDAP is flaw ervice.	N/A		O-CAN UBUN- 04041	-
N/A	05-03-2019	6.8	Multiple me corruption addressed with memory has is sue is fixe tvOS 12.1.2 iTunes 12.9 Windows, it windows 7 maliciously content magarbitrary co	issues w with imp ndling. I d in iOS , Safari 1 2.3 for Cloud fo .10. Prod crafted y lead to ode exec	roved This 12.1.3, 2.0.3, r cessing web ution.	N/A		O-CAN UBUN- 04041	-
N/A	05-03-2019	6.8	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.1.3, tvOS 12.1.2, Safari 12.0.3, iTunes 12.9.3 for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID: CVE-2019-6215		N/A		0-CAN UBUN- 04041		
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Dat	e CVSS	Descrip	tion & CV	E ID	Pa	atch	NCII	IPC ID
Carel									
pcoweb_card_	_firmware								
N/A	01-03-2019	5	The Glen I Deutschlar implement Carel pCOV configurate remote attraccess via on port 10 demonstrate moder (which is 1 reconfigurate mode" or 'CVE ID: C	nd GmbH tation of the Web ion tool a ackers to an HTTP 000, as ted by re in passwo .234), or ing "part vacation	the allows obtain session eading rd y mode."	N/A		O-CAF PCOW 04041	
chuango									
a11_pstn/lcd	/rfid_touch_a	alarm_sys	tem_firmw	are					
N/A	11-03-2019	6.4	The Chuan burglar-ali uses static remote cor an attacke or trigger remotely vattacks, as by Chuang products, a Chuango be products s Eminent E Alarm Syst	arm prod codes in ntrol, allo r to arm, the alarm ia replay demonst o brande and non- randed uch as th M8617 O	uct line the RF owing disarm, a crated d	N/A			J-A11 19/420
a8_pstn_alarn	n_system_fir	mware							
N/A	11-03-2019	6.4	The Chuar burglar-al	_		N/A		о-сни	J-A8_P-
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cro Denial of Servi	-			-				on; DoS-

system	_firmw	remote contan attacker or trigger the remotely via attacks, as do by Chuango products, are Chuango broducts su Eminent EM Alarm System CVE ID : CV	a replay demonstrated branded nd non- randed ach as the M8617 OV2 Wifi em. VE-2019-9659 go 433 MHz rm product line codes in the RF trol, allowing			04041	9/421
<u>system</u>	_firmw	The Chuang burglar-alar uses static c remote cont an attacker	go 433 MHz rm product line codes in the RF trol, allowing				
system		The Chuang burglar-alar uses static c remote cont an attacker	rm product line codes in the RF trol, allowing				
2019	6.4	remotely via attacks, as d by Chuango products, ar Chuango bra products su Eminent EM Alarm Syste	he alarm a replay demonstrated b branded nd non- randed ach as the M8617 OV2 Wifi em.	N/A		O-CHU AWV 04041	
arm_sys	stem_fi	•					
2019	6.4	The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay		N/A		O-CHU 04041	_
		2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10
	2019	2019 6.4	products su Eminent EM Alarm Syste CVE ID : CV arm_system_firmware The Chuang burglar-ala uses static of remote con an attacker or trigger th remotely vi	Alarm System. CVE ID: CVE-2019-9659 The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay	products such as the Eminent EM8617 OV2 Wifi Alarm System. CVE ID : CVE-2019-9659 The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay	products such as the Eminent EM8617 OV2 Wifi Alarm System. CVE ID : CVE-2019-9659 The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay	products such as the Eminent EM8617 OV2 Wifi Alarm System. CVE ID : CVE-2019-9659 The Chuango 433 MHz burglar-alarm product line uses static codes in the RF remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay O-CHU 04041

Vulnerability Type(s)	Publish Date	cvss	Descripti	ion & CVE I	D	Pa	tch	NCII	PC ID
			attacks, as d by Chuango products, an Chuango bra products sud Eminent EM Alarm Syste	branded ad non- anded ch as the 18617 OV2 m.	2 Wifi				
cg-105s_on-si	te_alarm_syste	n_firm	ware						
N/A	11-03-2019	6.4	The Chuange burglar-alar uses static contains attacker to trigger the remotely via attacks, as do by Chuango products, and Chuango braproducts such Eminent EM Alarm Syste	rm production odes in the crol, allow to arm, distending the alarm a replay emonstrated and non-anded ch as the 18617 OV2 m.	et line e RF ing sarm, ted	N/A			J-CG-1- 9/424
g3_gsm/sms_a	alarm_system_f	irmwa	re						
N/A	11-03-2019	6.4	The Chuang burglar-alar uses static coremote control an attacker to trigger the remotely via attacks, as doby Chuango products, and Chuango braproducts such products such as the chuango braction of	rm production odes in the crol, allow to arm, distending a replay emonstration branded and non-anded	et line e RF ing sarm,	N/A			J-G3_G- 9/425
CV Scoring Scale (CVSS)	e 0-1 1-	2 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 & CV	E ID	Pa	atch	NCI	IPC ID
			Eminent El	em.					
			CVE ID : CV		-9659				
g5_plus_gsm/	sms/rfid_tou	ch_alarm				1			
N/A	11-03-2019	6.4	The Chuang burglar-ala uses static remote con an attacker or trigger tremotely viattacks, as by Chuango products, a Chuango bi products su Eminent El Alarm Systems	rm prodes in trol, allo to arm, when alarm a replay demonst or branded and as the M8617 Or em.	uct line the RF wing disarm, rated d	N/A			J-G5_P- 19/426
			CVE ID : CV	E-2019	-9659				
g5w_3g_firmv	ware								
N/A	11-03-2019	6.4	The Chuang burglar-ala uses static remote con an attacker or trigger tremotely viattacks, as by Chuango products, a Chuango bi products su Eminent El Alarm Systems (CVE ID : CVE ID : CVE ID : CVE ID CVE ID	rm prodecodes in trol, allo to arm, when alarm a replay demonst oranded and as the M8617 Oran.	uct line the RF wing disarm, rated d	N/A		0-CHU G5W_ 04041	
Wifi/cellular_	_smart_home	_system_l	h4_plus_firn	iware		•		•	
CV Scoring Scal (CVSS)	e 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cros Denial of Servic	_			-				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patc	h	NCII	PC ID
N/A	11-03-2019	6.4	The Chuango 433 MHz burglar-alarm product linuses static codes in the RF remote control, allowing an attacker to arm, disarm or trigger the alarm remotely via replay attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the Eminent EM8617 OV2 Wi Alarm System. CVE ID: CVE-2019-9659	n, N/A			J-WIFI- 9/428
wifi_alarm_sy	stem_firmwar	9		<u>'</u>			
N/A	11-03-2019	6.4	The Chuango 433 MHz burglar-alarm product linuses static codes in the RF remote control, allowing an attacker to arm, disarm or trigger the alarm remotely via replay attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the Eminent EM8617 OV2 Wi Alarm System.	n, N/A			J-WIFI- 9/429
Cisco							
Nx-os							
N/A	06-03-2019	7.2	A vulnerability in the controller authorization functionality of Cisco	N/A		0-CIS- 04041	NX-0- 9/430

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escalate standard users with root privilege on an affected device. The vulnerability is due to a misconfiguration of certain sudoers files for the bashroot component on an affected device. An attacker could exploit this vulnerability by authenticating to the affected device with a crafted user ID, which may allow temporary administrative access to escalate privileges. A successful exploit could allow the attacker to escalate privileges on an affected device. This Vulnerability has been fixed in version 4.0(1h) CVE ID: CVE-2019-1585		
N/A	06-03-2019	2.1	A vulnerability in the Cisco Nexus 9000 Series Fabric Switches running in Application-Centric Infrastructure (ACI) mode could allow an authenticated, local attacker to read arbitrary files on an affected device. The vulnerability is due to a lack of proper input and	N/A	O-CIS-NX-O- 040419/431

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			validation checking mechanisms of usersupplied input sent to an affected device. A successful exploit could allow the attacker unauthorized access to read arbitrary files on an affected device. This vulnerability has been fixed in version 14.0(1h). CVE ID: CVE-2019-1588		
N/A	06-03-2019	7.2	A vulnerability in a specific CLI command implementation of Cisco Nexus 9000 Series ACI Mode Switch Software could allow an authenticated, local attacker to escape a restricted shell on an affected device. The vulnerability is due to insufficient sanitization of user-supplied input when issuing a specific CLI command with parameters on an affected device. An attacker could exploit this vulnerability by authenticating to the device CLI and issuing certain commands. A successful exploit could allow the attacker to escape the restricted shell and execute arbitrary commands with root-level	N/A	O-CIS-NX-O- 040419/432

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			privileges on the affected device. This vulnerability only affects Cisco Nexus 9000 Series ACI Mode Switches that are running a release prior to 14.0(3d). CVE ID: CVE-2019-1591		
N/A	06-03-2019	7.2	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level by executing commands authorized to other user roles. The attacker must authenticate with valid user credentials. The vulnerability is due to the incorrect implementation of a Bash shell command that allows role-based access control (RBAC) to be bypassed. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level by executing commands that should be restricted to other roles. For example, a dev-ops user could	N/A	O-CIS-NX-O- 040419/433

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			escalate their privilege level to admin with a successful exploit of this vulnerability.		
			CVE ID : CVE-2019-1593		
N/A	06-03-2019	6.1	A vulnerability in the 802.1X implementation for Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to incomplete input validation of Extensible Authentication Protocol over LAN (EAPOL) frames. An attacker could exploit this vulnerability by sending a crafted EAPOL frame to an interface on the targeted device. A successful exploit could allow the attacker to cause the Layer 2 (L2) forwarding process to restart multiple times, leading to a system-level restart of the device and a DoS condition. Note: This vulnerability affects only NX-OS devices configured with 802.1X functionality. Cisco Nexus 1000V Switch for VMware vSphere devices are affected in versions prior to	N/A	O-CIS-NX-O- 040419/434

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			5.2(1)SV3(1.4b). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.3(5)N1(1) and 7.1(5)N1(1b). Nexus 7000 and 7700 Series Switches are affected in versions prior to 8.2(3). Nexus 9000 Series Fabric Switches in ACI Mode are affected in versions prior to 13.2(1l). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4). CVE ID: CVE-2019-1594		
N/A	06-03-2019	6.1	A vulnerability in the Fibre Channel over Ethernet (FCoE) protocol implementation in Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an incorrect allocation of an internal interface index. An adjacent attacker with the	N/A	O-CIS-NX-O- 040419/435

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			ability to submit a crafted FCoE packet that crosses affected interfaces could trigger this vulnerability. A successful exploit could allow the attacker to cause a packet loop and high throughput on the affected interfaces, resulting in a DoS condition. This vulnerability has been fixed in version 7.3(5)N1(1). CVE ID: CVE-2019-1595		
N/A	07-03-2019	7.2	A vulnerability in the Bash shell implementation for Cisco NX-OS Software could allow an authenticated, local attacker to escalate their privilege level to root. The attacker must authenticate with valid user credentials. The vulnerability is due to incorrect permissions of a system executable. An attacker could exploit this vulnerability by authenticating to the device and entering a crafted command at the Bash prompt. A successful exploit could allow the attacker to escalate their privilege level to root. Nexus 3000 Series Switches are affected in versions prior to	N/A	0-CIS-NX-0- 040419/436

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1596		
N/A	07-03-2019	7.8	Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The	N/A	O-CIS-NX-O- 040419/437

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			LDAP packet must have a		
			source IP address of an		
			LDAP server configured on		
			the targeted device. A		
			successful exploit could		
			cause the affected device		
			to reload, resulting in a		
			DoS condition. Firepower		
			4100 Series Next-		
			Generation Firewalls are		
			affected in versions prior		
			to 2.0.1.201, 2.2.2.54, and		
			2.3.1.75. Firepower 9300		
			Security Appliances are		
			affected in versions prior		
			to 2.0.1.201, 2.2.2.54 and		
			2.3.1.75. MDS 9000 Series		
			Multilayer Switches are		
			affected in versions prior		
			to 8.2(1). Nexus 3000		
			Series Switches are		
			affected in versions prior		
			to 7.0(3)I7(1). Nexus 3500		
			Platform Switches are		
			affected in versions prior		
			to 7.0(3)I7(2). Nexus 7000		
			and 7700 Series Switches		
			are affected in versions		
			prior to 8.2(1). Nexus		
			9000 Series Switches in		
			Standalone NX-OS Mode		
			are affected in versions		
			prior to 7.0(3)I7(1). Cisco		
			UCS 6200 and 6300 Fabric		
			Interconnect devices are		
			affected in versions prior		
			to 3.2(2b).		
			CVE ID : CVE-2019-1597		

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

Multiple vulnerabilities in the implementation of the Lightweight Directory Access Protocol (LDAP) feature in Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause an affected device to reload, resulting in a denial of service (DoS) condition. The vulnerabilities are due to the improper parsing of LDAP packets by an affected device. An attacker could exploit these vulnerabilities by sending an LDAP packet crafted using Basic Encoding Rules (BER) to an affected device. The LDAP packet must have a source IP address of an LDAP server configured on the targeted device. A successful exploit could cause the affected device to reload, resulting in a DoS condition. Firepower 4100 Series Next-Generation Firewalls are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. Firepower 9300 Security Appliances are affected in versions prior to 2.0.1.201, 2.2.2.54, and 2.3.1.75. MDS 9000 Series	Vulnerability Type(s)	Publish Date	cvss	Descrip	ion & CV	E ID	Pa	itch	NCII	PC ID
- III I I I I I I I I I I I I I I I I I	N/A	07-03-2019	7.8	the implemental Lightweigh Access Prote feature in Construction of Software and Software consulting in attacker to affected development of the improperation of the improperation of the improperation of the service (Don The vulners to the improperation of the improperation of the improperation of the improperation of the service of these vulners and affected development of the targeted source IP and LDAP served the targeted successful of the cause the accessful of the improperation of the improvement of	entation to Directo cocol (LE isco FXC) and Cisco ould allow cause and isco could allow cause and isco per partice. An allow cause and isco per partice. And allow cause and isco per partice. And allow cause (BE) device. The configuration of	of the ory OAP) OS NX-OS w an emote of eload, l of tion. are due rsing of oit is by acket CR) to The nave a f an ured on A ould levice in a power ls are prior 4, and elevice in a power 4, and elevice	N/A			
(5455)	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)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Multilayer Switches are affected in versions prior to 8.2(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(2). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(20), 7.3(2)D1(1), and 8.2(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I7(1). UCS 6200 and 6300 Fabric Interconnect are affected in versions prior to 3.2(2b). CVE ID: CVE-2019-1598		
N/A	07-03-2019	7.8	A vulnerability in the network stack of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on the affected device. The vulnerability is due to an issue with allocating and freeing memory buffers in the network stack. An attacker could exploit this vulnerability by sending crafted TCP streams to an affected device in a sustained way. A	N/A	0-CIS-NX-0- 040419/439

Vulnerability Type(s)	Publish Date	cvss	Descri	ption & CVI	ID	Pa	tch	NCII	PC ID
			successfu	exploit co	ould				
			cause the	network s	tack of				
			an affecte	d device to	run				
			out of ava	ilable buff	ers,				
			impairing	operation	s of				
			control pl	ane and					
			managem	ent plane					
			protocols						
			DoS cond	DoS condition. Note: This					
			vulnerabi	lity can be					
			triggered	only by tra	affic				
			that is des	tined to a	n				
			affected d	evice and	cannot				
			be exploit	ed using t	raffic				
			that trans	its an affe	cted				
			device. Ne	xus 1000	J				
			Switch for	Microsof	t				
			Hyper-V i	s affected :	in				
			versions p	rior to					
			5.2(1)SM:	3(2.1). Nex	tus				
			1000V Sw	ritch for VI	Mware				
			vSphere is	s affected i	n				
			versions p	rior to					
			5.2(1)SV3	(4.1a). Ne	xus				
			3000 Seri	es Switche	es are				
			affected in	versions	prior				
			to 7.0(3)I	7(6) and 9	.2(2).				
			Nexus 350	00 Platfori	n				
			Switches	are affecte	d in				
			versions p	rior to					
			6.0(2)A8(11), 7.0(3)17(6),				
			and 9.2(2)). Nexus 3	500				
			Platform :	Switches a	re				
			affected in						
			to 7.0(3)F						
			Nexus 550						
			6000 Seri	es Switche	es are				
			affected in	versions	prior				
			to 7.1(5)N	11(1b) and					
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
			7.3(5)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22. Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5) and 9.2(2). UCS 6200 and 6300 Series Fabric Interconnect are affected in versions prior to 3.2(3j) and 4.0(2a). UCS 6400 Series Fabric Interconnect are affected in versions prior to 4.0(2a).		
N/A	07-03-2019	2.1	A vulnerability in the file system permissions of Cisco FXOS Software and Cisco NX-OS Software could allow an authenticated, local attacker to access sensitive information that is stored in the file system of an affected system. The vulnerability is due to improper implementation of file system permissions. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow the attacker to access sensitive and critical files. Firepower	N/A	O-CIS-NX-O- 040419/440

Vulnerability Type(s)	Publish Dat	te CVSS	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID
			4100 Series	Next-					
			Generation	Firewal	ls are				
			affected in	versions	prior				
			to 2.2.2.91	and 2.3.1	1.110.				
			Firepower	9300 Sei	ries				
			Next-Gener	ation Fi	rewalls				
			are affected	l in versi	ons				
			prior to 2.2						
			2.3.1.110. N	1DS 900	0 Series				
			Multilayer	Switches	are				
			affected in	versions	prior				
			to 6.2(25),	8.1(1b),	and				
			8.3(1). Nex	us 3000	Series				
			Switches ar	e affecte	ed in				
			versions pr						
			7.0(3)I4(9)	and					
			7.0(3)17(4)	. Nexus 3	3500				
			Platform Sv	vitches a	ıre				
			affected in	versions	prior				
			to 6.0(2)A8	(10) and	i				
			7.0(3)I7(4)						
			Platform Sv						
			affected in		•				
			to 7.0(3)F3						
			2000, 5500						
			6000 Series						
			affected in		•				
			to 7.1(5)N1	` ,					
			7.3(3)N1(1						
			and 7700 S						
			are affected		ons				
			prior to 6.2	. ,.					
			7.3(3)D1(1		2(3).				
			Nexus 9000						
			Switches-S						
			affected in		prior				
			to 7.0(3)I4		25005				
			7.0(3)17(4)						
			Series Line Cards and						
CV Scoring Scale (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Typ			st Forgery; Dir. s Site Scripting;		-				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
-	Publish Date 08-03-2019	7.2	Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1600 A vulnerability in the filesystem permissions of Cisco NX-OS Software could allow an authenticated, local attacker to gain read and write access to a critical configuration file. The vulnerability is due to a failure to impose strict filesystem permissions on the targeted device. An attacker could exploit this vulnerability by accessing and modifying restricted files. A successful exploit could allow an attacker to use the content of this configuration file to bypass authentication and log in as any user of the device. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series	Patch N/A	O-CIS-NX-O-040419/441
			to 6.2(25), 8.1(1b), and		

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(1b) and 7.3(3)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID : CVE-2019-1601		
N/A	08-03-2019	4.6	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to escalate lower-level privileges to the administrator level. The vulnerability is due to insufficient authorization enforcement. An attacker could exploit this vulnerability by authenticating to the targeted device and executing commands that could lead to elevated	N/A	O-CIS-NX-O- 040419/442

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			privileges. A successful exploit could allow an attacker to make configuration changes to the system as administrator. Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1603		
N/A	08-03-2019	7.2	A vulnerability in the user account management interface of Cisco NX-OS Software could allow an authenticated, local attacker to gain elevated privileges on an affected device. The vulnerability is due to an incorrect authorization check of user accounts and their associated Group ID (GID). An attacker could exploit this vulnerability by taking	N/A	O-CIS-NX-O- 040419/443

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			advantage of a logic error that will permit the use of higher privileged commands than what is necessarily assigned. A successful exploit could allow an attacker to execute commands with elevated privileges on the underlying Linux shell of an affected device. Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 8.2(3), and 8.3(2). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches-Standalone are affected in versions prior to 7.0(3)I7(4). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5).		
N/A	08-03-2019	7.2	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, local attacker to execute	N/A	O-CIS-NX-O- 040419/444

Vulnerability Type(s)	Publish Dat	te CVSS	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
			arbitrary co	de as ro	ot. The				
			vulnerabilit	y is due	to				
			incorrect in	put vali	dation				
			in the NX-A	PI featu	re. An				
			attacker co	ıld expl	oit this				
			vulnerabilit	y by sen	iding a				
			crafted HTT	P or HT	TPS				
			request to a						
			service on a						
			device that		NX-API				
			feature ena						
			successful e	-					
			allow the at						
			a buffer ove						
			execute arb	•					
			root. Note:						
			feature is d		•				
			default. MD						
			Multilayer S						
			affected in		-				
			to 8.1(1). N		00				
			Series Swite						
			affected in		prior				
			to 7.0(3)I4(2500				
			7.0(3)I7(1)						
			Platform Sv						
			affected in		•				
			to 6.0(2)A8	` ,					
			3600 Platfo						
			are affected						
			prior to 7.0	. ,					
			Nexus 2000						
			and 6000 S						
			are affected						
			prior to 7.3		-				
			Nexus 7000 Series Swite		UU				
					nrior				
			affected in to 7.3(3)D1		•				
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 Typ	pe(s): CSRF- Cro	ss Site Reque	st Forgery; Dir.	Γrav Dire	ectory Trav	ersal; +In	fo- Gain I	nformatio	n; DoS-
, ,		-	s Site Scripting;		=				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1605		
N/A	08-03-2019	7.2	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 7000	N/A	O-CIS-NX-O- 040419/445

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). CVE ID: CVE-2019-1607 A vulnerability in the CLI		
N/A	08-03-2019	7.2	of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(1). Nexus 7000 and 7700 Series Switches	N/A	O-CIS-NX-O- 040419/446

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
Type(s)			are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). CVE ID: CVE-2019-1608 A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local		
N/A	08-03-2019	7.2	attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(27), 8.1(1b), and 8.3(2). Nexus 3500 Platform Switches are affected in versions prior	N/A	O-CIS-NX-O- 040419/447

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			to 7.0(3)I7(6). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected in versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3), and 8.3(2). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected in versions prior to 7.0(3)I4(9) and7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected in versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1609		
N/A	11-03-2019	7.2	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including	N/A	O-CIS-NX-O- 040419/448

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			malicious input as the argument of an affected command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3500 Platform Switches and Nexus 3000 Series Switches software versions prior to 7.0(3)17(4) are affected.		
N/A	11-03-2019	7.2	A vulnerability in the CLI of Cisco NX-OS Software and Cisco FXOS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful	N/A	O-CIS-NX-O- 040419/449

Vulnerability Type(s)	Publish Da	te CVSS	Descript	ion & CV	E ID	Pa	tch	NCII	PC ID	
			exploit coul	d allow	the					
			attacker to	execute						
			arbitrary co	mmand	s on					
			the underly	ing oper	ating					
			system with	ı elevate	ed					
			privileges. A	An attacl	ker					
			would need	valid						
			administrat	or crede	entials					
			to exploit th	nis						
			vulnerabilit	-	ower					
			4100 Series	Next-						
			Generation	Firewal	ls are					
			affected rur	ning so	ftware					
			versions pr	ior to 2.2	2.2.91,					
			2.3.1.110, a	nd 2.4.1	.222.					
			Firepower (9300 Sed	curity					
			Appliance a	re affect	ted					
			running sof	tware ve	ersions					
			prior to 2.2	.2.91, 2.3	3.1.110,					
			and 2.4.1.22	22. MDS	9000					
			Series Mult	-						
			are affected							
			software ve	•						
			6.2(25) and							
			3000 Series							
			affected rur	O	ftware					
			versions pr							
			7.0(3)I4(9)							
			7.0(3)17(5)							
			Platform Sv							
			affected rur	Ü	ftware					
			versions pr							
			7.0(3)17(5)							
			Platform Sv							
			affected rur	_	ftware					
			versions pr							
			7.0(3)F3(5)							
			5500, 5600		υO					
			Series Switches are							
CV Scoring Scale (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Vulnerability Ty	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; DoS-									
, ,	Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Info- Gain Information; Dos- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.									

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			affected running software versions prior to 7.1(5)N1(1b) and 7.3(4)N1(1). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22), 7.3(3)D1(1), 8.2(3). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(5). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1611		
N/A	11-03-2019	7.2	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient validation of arguments passed to certain CLI commands. An attacker could exploit this vulnerability by including malicious input as the argument of an affected command. A successful	N/A	O-CIS-NX-O- 040419/450

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to execute arbitrary commands on the underlying operating system with elevated privileges. An attacker would need valid administrator credentials to exploit this vulnerability. Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)I7(4). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Stand are affected running software versions prior to 7.0(3)F3(5). CVE ID: CVE-2019-1612		
N/A	11-03-2019	4.6	A vulnerability in the CLI of Cisco NX-OS Software could allow an authenticated, local attacker to execute arbitrary commands on the underlying operating system of an affected device. The vulnerability is due to insufficient	N/A	O-CIS-NX-O- 040419/451

		te CVS	3	Description & CVE ID				tch	INCII	PC ID
			val	idation o	of argum	ents				
			pas	sed to c	ertain CI	LI				
			cor	nmands.	An atta	cker				
			cou	ıld explo	it this					
			vul	nerabilit	ty by inc	luding				
			ma	licious ii	nput as t	he				
			arg	ument o	f an affe	cted				
			cor	nmand.	A succes	sful				
			exp	oloit coul	ld allow	the				
			atta	acker to	execute					
			arb	itrary co	ommand	ls on				
			the	underly	ring oper	rating				
			sys	tem witl	n elevate	ed				
			pri	vileges. <i>I</i>	An attacl	ker				
			wo	uld need	l valid					
			adr	ninistrat	tor crede	entials				
				exploit tl						
			vul	nerabilit	y. MDS ⁹	9000				
			Ser	ies Mult	ilayer Sv	witches				
			are	affected	l runnin	g				
				tware ve	_					
				(27) and						
			300	00 Series	Switch	es are				
				ected rui		ftware				
				sions pr						
				(3)14(9)						
				(3)17(6)						
				tform Sv						
			affe	ected rui	nning so	ftware				
				sions pr						
				(2)A8(1	-					
				(3)17(6)						
				tform Sv		_				
				ected rui	Ü	ftware				
				sions pr						
				(3)F3(5)		9000				
				ies Swit						
				ndalone						
			are affected running							
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 Typ	e(s): CSRF- Cro Denial of Serv	-				-				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			software versions prior to 7.0(3)I4(9), 7.0(3)I7(6). Nexus 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 6.2(22) and 8.2(3). CVE ID: CVE-2019-1613		
N/A	11-03-2019	9	A vulnerability in the NX-API feature of Cisco NX-OS Software could allow an authenticated, remote attacker to execute arbitrary commands with root privileges. The vulnerability is due to incorrect input validation of user-supplied data by the NX-API subsystem. An attacker could exploit this vulnerability by sending malicious HTTP or HTTPS packets to the management interface of an affected system that has the NX-API feature enabled. A successful exploit could allow the attacker to perform a command-injection attack and execute arbitrary commands with root privileges. Note: NX-API is disabled by default. MDS	N/A	O-CIS-NX-O- 040419/452

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
			9000 Series Multilayer Switches are affected running software versions prior to 8.1(1b) and 8.2(3). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)I7(4). Nexus 2000, 5500, 5600, and 6000 Series Switches are affected running software versions prior to 7.3(4)N1(1). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 7000 and 7700 Series Switches are affected running software versions prior to 7.3(3)D1(1) and 8.2(3).		
			CVE ID : CVE-2019-1614		
N/A	11-03-2019	4.6	A vulnerability in the Image Signature Verification feature of Cisco NX-OS Software could allow an authenticated, local attacker with administrator-level credentials to install a	N/A	O-CIS-NX-O- 040419/453

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			malicious software image		
			on an affected device. The		
			vulnerability is due to		
			improper verification of		
			digital signatures for		
			software images. An		
			attacker could exploit this		
			vulnerability by loading an		
			unsigned software image		
			on an affected device. A		
			successful exploit could		
			allow the attacker to boot		
			a malicious software		
			image. Note: The fix for		
			this vulnerability requires		
			a BIOS upgrade as part of		
			the software upgrade. For		
			additional information, see		
			the Details section of this		
			advisory. Nexus 3000		
			Series Switches are		
			affected running software		
			versions prior to		
			7.0(3)I7(5). Nexus 9000		
			Series Fabric Switches in		
			ACI Mode are affected		
			running software versions		
			prior to 13.2(1l). Nexus		
			9000 Series Switches in		
			Standalone NX-OS Mode		
			are affected running		
			software versions prior to		
			7.0(3)I7(5). Nexus 9500 R-		
			Series Line Cards and		
			Fabric Modules are		
			affected running software		
			versions prior to		
			7.0(3)F3(5).		

 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-2019-1615		
N/A	11-03-2019	5	A vulnerability in the Cisco Fabric Services component of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a buffer overflow, resulting in a denial of service (DoS) condition. The vulnerability is due to insufficient validation of Cisco Fabric Services packets. An attacker could exploit this vulnerability by sending a crafted Cisco Fabric Services packet to an affected device. A successful exploit could allow the attacker to cause a buffer overflow, resulting in process crashes and a DoS condition on the device. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25), 8.1(1b), 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)14(9) and 7.0(3)17(4). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(10) and	N/A	O-CIS-NX-O- 040419/454

 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 D	ate	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID										
				7.0(3)I7(4) Platform Sv affected run versions pr 7.0(3)F3(5) and 7700 S are affected software ve 6.2(22) and 9000 Series Standalone are affected software ve 7.0(3)I4(9) 7.0(3)I7(4) Series Line Fabric Mod affected run versions pr 7.0(3)F3(5) 6300, and 6 Interconner running soft prior to 3.2 4.0(2a). CVE ID: CV	vitches anning so ior to Nexus frunning ersions pand Nexus frunning ersions pand Nexus frunds are uning so ior to O. UCS 626400 Fabots are a ftware version and frunds are a ftware versions and ftware versions pand Nexus frunds are a ftware versions are a ftware versions and ftware versions are a ftware versions and ftware versions and ftware versions are a ftware versions and a ftware versions are a ftware versions are a ftware versions and a ftware versions are a ftware versions are a ftware versions and a ftware versions and a ftware versions are a	ftware ftware 7000 ritches g orior to Nexus es in Mode g orior to 9500 R- nd ftware 200, oric ffected ersions														
application_p	olicy_intra	astruc	ture_c				1		1											
N/A	06-03-20	19	7.2	A vulnerable controller a functionality Nexus 9000 Mode Switch could allow authenticate attacker to standard us privilege or device. The	N/A		O-CIS- 04041	APPL- 9/455												
CV Scoring Scale (CVSS)	e 0-1	1-2	2 2	3-4	4-5	5-6	6-7	7-8	8-9	9-10										
			_			_			nformatio	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.										

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID		
			sconfigured deviced deviced deviced deviced deviced by sing to the vice with r ID, whice acception acception to the vileges of vice. This ty has besion 4.00 vice vileges of vice acception 4.00 vice wileges of vice acception 4.00 vice acception 4.00 vice vice acception 4.00 vice vice acception 4.00 vice vice vice vice vice vice vice vice	iles for onent ce. An oit this e a ch may ss to A ould oo on an seen (1h)							
Debian			CVE ID . CV	E-2017	-1303						
Mebian_linux A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service. CVE ID: CVE-2019-3824											
N/A	08-03-2019	5	An issue wa PHP before before 7.2.1 before 7.3.3	N/A			3-DEBI- 9/457				
CV Scoring Scal (CVSS) Vulnerability Ty	0-1		2-3 3-4 st Forgery; Dir.	4-5 Trav Dire	5-6	6-7 ersal; +In	7-8 fo- Gain Ir	8-9	9-10 on; DoS-		
	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)	Р	ublish Da	ite	cvss	Descrip	Pa	itch	NCII	IPC ID		
					way renaming filesystems implement that file be briefly available wrong period the rename thus enabling unauthorizaccess the course of the cou						
					An issue w						
N/A	08	-03-201	9	7.5	the EXIF con PHP before 7.2. before 7.3. uninitialized exif_process RNOTE becomishandling maker_not	the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKE RNOTE because of mishandling the maker_note->offset relationship to value_len.					3-DEBI- 19/458
N/A	08	-03-201	9	7.5	An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF. CVE ID: CVE-2019-9641			N/A			3-DEBI- 19/459
eminent											
em8617_ov2_	wifi	i_alarm	_syst	em_fir	mware						
N/A	11	-03-201	9	6.4	The Chuan burglar-ala uses static	N/A		O-EM EM86 04041			
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 Ty				_	st Forgery; Dir. s Site Scripting;	Sql- SQL Ir	_			nformatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			remote control, allowing an attacker to arm, disarm, or trigger the alarm remotely via replay attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the Eminent EM8617 OV2 Wifi Alarm System. CVE ID: CVE-2019-9659		
Fujitsu					
gk900_firmw	are				
N/A	15-03-2019	5.8	The receiver (aka bridge) component of Fujitsu Wireless Keyboard Set LX901 GK900 devices allows Keystroke Injection. This occurs because it accepts unencrypted 2.4 GHz packets, even though all legitimate communication uses AES encryption. CVE ID: CVE-2019-9835	N/A	O-FUJ-GK90- 040419/461
lx901_firmwa	ire				
N/A	15-03-2019	5.8	The receiver (aka bridge) component of Fujitsu Wireless Keyboard Set LX901 GK900 devices allows Keystroke Injection. This occurs because it accepts unencrypted 2.4 GHz packets, even though all legitimate	N/A	O-FUJ-LX90- 040419/462

 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
			communication uses AES		
			encryption.		
			CVE ID : CVE-2019-9835		
Korenix					
jetport_5601	_firmware				
N/A	12-03-2019	4.3	The Web manager (aka Commander) on Korenix JetPort 5601 and 5601f devices has Persistent XSS via the Port Alias field under Serial Setting. CVE ID: CVE-2019-9725	N/A	O-KOR-JETP- 040419/463
jetport_5601	f_firmware				
N/A	12-03-2019	4.3	The Web manager (aka Commander) on Korenix JetPort 5601 and 5601f devices has Persistent XSS via the Port Alias field under Serial Setting. CVE ID: CVE-2019-9725	N/A	O-KOR-JETP- 040419/464
Linux			0.2.2.0.2.20.2.7.7.20		
linux_kernel					
N/A	05-03-2019	4.9	In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.	N/A	O-LIN-LINU- 040419/465

CV Scoring Scale	0.1	1.2	2.2	2.4	1-5	5.6	6.7	70	9.0	9-10
(CVSS)	0-1	1-2	2-5	3-4	4-3	3-0	0-7	7-0	0-3	3-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9213		
Microsoft					
windows_10					
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0595	O-MIC- WIND- 040419/466
			CVE ID : CVE-2019-0595		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0596	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0596	O-MIC- WIND- 040419/467
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad	O-MIC- WIND- 040419/468

Vulnerability Type(s)	Publish Date	cvss		Descript	tion & CV	E ID	Pa	tch	NCIII	PC ID
			Cod Vuli is ui 059 CVE 201 062	Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019- 0595, CVE-2019-0596, CVE-2019-0598, CVE- 2019-0599, CVE-2019- 0625. CVE ID: CVE-2019-0597				/CVE- 0597		
N/A	05-03-2019	9.3	vulr the Eng obje Data Cod Vulr is ur 059 CVE 201 062	nerability Windownine impects in malabase Execunerability of the control of the c	nemory, ngine Re	when tabase handles aka 'Jet emote CVE ID -2019- 96, 'E- 19-	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC- WIND- 04041	
N/A	05-03-2019	9.3	vulr the Eng obje Data Cod Vulr is ur 059 CVE 201 062	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625. CVE ID: CVE-2019-0599		al.msr osoft.c	com/en ecurity- nce/ad /CVE-	O-MIC- WIND- 04041		
CV Scoring Scale	9 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	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0600	O-MIC- WIND- 040419/471
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600. CVE ID: CVE-2019-0601	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0601	O-MIC- WIND- 040419/472
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0602	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0602	O-MIC- WIND- 040419/473

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0615	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0615	O-MIC- WIND- 040419/474
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0616	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0616	O-MIC- WIND- 040419/475
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0618	O-MIC- WIND- 040419/476

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			0662.		
			CVE ID : CVE-2019-0618		
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0660, CVE-2019-0664.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0619	O-MIC- WIND- 040419/477
			CVE ID : CVE-2019-0619		
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663. CVE ID: CVE-2019-0621	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0621	O-MIC- WIND- 040419/478
N/A	05-03-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0623	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0623	O-MIC- WIND- 040419/479

			te	CVSS	A remote code execution				Patch		NCIIPC ID		
N/A	05-03	3-201	9	9.3	vuln the Eng obje Dat Cod Vuln is un 059 CVE 201	nerabili Windov gine imp ects in n abase E le Execu nerabili nique fr 5, CVE- 2-2019- 9-0598	ty exists vs Jet Da roperly nemory, ngine Re	when atabase handles aka 'Jet emote CVE ID 5-2019-596, VE-019-	al.msi osoft. -US/s guida	//port com/en ecurity- nce/ad r/CVE-			
N/A	05-03	3-201	9	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.				al.msi osoft. -US/s guida	//port c.micr com/en ecurity- nce/ad r/CVE-	O-MIC WIND 04041		
N/A	05-03	3-201	9	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-2019-0632. CVE ID: CVE-2019-0627				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0627				
N/A	05-03	3-201	9	2.1	An information disclosure vulnerability exists when				_	//port c.micr	O-MIC- WIND-		
CV Scoring Scale (CVSS) Vulnerability Typ		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

			the win32k improperly kernel infor 'Win32k Info Disclosure	provides			om/en	04041	0./402
			CVE ID : CV	Vulnerab	n ility'.	guidan visory 2019-0	/CVE-		7/4 83
N/A 05-	03-2019	9	A remote covulnerability way that the Server Mess (SMBv2) secretain requivers of Sunday Sunda		c.micr om/en curity- ice/ad /CVE-	O-MIC WIND- 04041	-		
N/A 05-	03-2019	4.6	A security for vulnerability Windows we allow an attraction bypass Devive Windows Structure Bypass Vulnerability CVE ID is under CVE-2019-0632. CVE ID: CVE I	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0631		O-MIC WIND- 04041	-		
N/A 05-	03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0632			
CV Scoring Scale (CVSS) Vulnerability Type(s):	0-1 1-2		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Pı	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCI	IPC ID	
					201	19-0631	0627, CV Y E-2019						
N/A	05-	03-201	9	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630. CVE ID: CVE-2019-0633				al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad /CVE- 0633	cr /en O-MIC- ity- WIND- ad 040419/ E-		
N/A	05-	03-201	9	5.5	An vult Wir hos to p from a system Hyp	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'.				//port c.micr com/en ecurity- nce/ad /CVE- 0635			
N/A	05-	03-201	9	2.1	vuli Wir disc aka Disc	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'. CVE ID: CVE-2019-0636			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0636		n O-MIC- - WIND-		
N/A	05-	03-201	9	5	A security feature bypass vulnerability exists when Windows Defender			https://port al.msrc.micr osoft.com/en		WIND-			
CV Scoring Scale (CVSS)	е	0-1 CSRF- Cro	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
			Firewall incorrectly applies firewall profiles to cellular network connections, aka 'Windows Defender Firewall Security Feature Bypass Vulnerability'. CVE ID: CVE-2019-0637	-US/security- guidance/ad visory/CVE- 2019-0637	
N/A	05-03-2019	6.9	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0656	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0656	O-MIC- WIND- 040419/491
N/A	05-03-2019	4.4	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0659	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0659	O-MIC- WIND- 040419/492
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0660	O-MIC- WIND- 040419/493

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID		
			CVE-2019-0664. CVE ID : CVE-2019-0660				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662	Inerability exists in the ay that the Windows raphics Device Interface (DI) handles objects in e memory, aka 'GDI+ emote Code Execution ulnerability'. This CVE ID unique from CVE-2019-662			
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0663	O-MIC- WIND- 040419/495		
			CVE ID : CVE-2019-0663				
windows_7				https://wawt			
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution		O-MIC- WIND- 040419/496		
CV Scoring Scale	e 0-1 1	-2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		
(CVSS) Vulnerability Ty			st Forgery; Dir. Trav Directory Tra				

Vulnerability Type(s)	Publi	sh Da	te	cvss		Descrip	tion & CV	E ID	Pa	itch	NCI	IPC ID
					is u 059 CVE 201 062	nique fr 96, CVE- E-2019- 9-0599 25.	ty'. This om CVE 2019-05 0598, CV , CVE-20	-2019- 197, 7E- 119-				
N/A	05-03	-201	9	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0596				al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad r/CVE- 0596	O-MIC WIND 04042	
N/A	05-03	-201	9	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0597				al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad r/CVE- 0597	O-MIC WIND 04042	
N/A	05-03	-201	9	9.3	A remote code execution vulnerability exists when				https://port al.msrc.micr		O-MIC- WIND-	
CV Scoring Scale)-1		2 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) Pa	tch	NCIIP	C ID
			the Windows Jet Datab Engine improperly har objects in memory, aka Database Engine Remo Code Execution Vulnerability'. This CV is unique from CVE-20 0595, CVE-2019-0596 CVE-2019-0597, CVE- 2019-0599, CVE-2019- 0625.	ndles -US/se guidar visory 2019-0	/CVE-	040419	9/499
			CVE ID : CVE-2019-05			 	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Datable Engine improperly hard objects in memory, akan Database Engine Remote Code Execution Vulnerability'. This CV is unique from CVE-200595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0598, CVE-2019-0598.	https://al.msr.osoft.c e ID US/seguidar visory, 2019-0	c.micr com/en ecurity- nce/ad /CVE-	O-MIC- WIND- 040419	
N/A	05-03-2019	1.9	An information disclos vulnerability exists who the Human Interface Devices (HID) componimproperly handles objects in memory, aka 'HID Information Disclosure Vulnerability This CVE ID is unique for CVE-2019-0601. CVE ID: CVE-2019-060	https://al.msrcosoft.ca -US/seguidarty'. visory	c.micr com/en ecurity- nce/ad /CVE-	O-MIC- WIND- 040419	
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	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	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0601	O-MIC- WIND- 040419/502
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0602	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0602	O-MIC- WIND- 040419/503
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0660,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0615	O-MIC- WIND- 040419/504

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID
			CVE-2019-	0664.					
			CVE ID : CV	/E-2019	-0615				
N/A	05-03-2019	4.3	An information vulnerabilithe Window component discloses the its memory GDI Informatics Disclosure This CVE III CVE-2019-2019-0615 0619, CVE-2019-CVE ID: CVE	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041			
N/A	05-03-2019	9.3	A remote c vulnerabili way that the Graphics D (GDI) hand the memore Remote Co Vulnerabili is unique fro 0662.	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041			
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-			-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
vuinerability Ty	pe(s): CSRF- Cross Denial of Service;	_		Sql- SQL In	_			ntormatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2019-0615, CVE-2019- 0616, CVE-2019-0660, CVE-2019-0664. CVE ID : CVE-2019-0619		
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663. CVE ID: CVE-2019-0621	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0621	O-MIC- WIND- 040419/508
N/A	05-03-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0623	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0623	O-MIC- WIND- 040419/509
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0625	O-MIC- WIND- 040419/510

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			0599. CVE ID : CVE-2019-0625		
N/A	05-03-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. CVE ID: CVE-2019-0626	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0626	O-MIC- WIND- 040419/511
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0628	O-MIC- WIND- 040419/512
N/A	A remote code vulnerability et way that the M Server Message (SMBv2) server certain request 'Windows SMB Code Execution Vulnerability'.' is unique from 0633.			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0630	O-MIC- WIND- 040419/513
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0	https://port al.msrc.micr osoft.com/en -US/security-	O-MIC- WIND- 040419/514

Vulnerability Type(s)	Publish Date	cvss	Descriptio	n & CVE ID	Pa	itch	NCII	PC ID
			(SMBv2) serve certain reques 'Windows SM Code Execution Vulnerability is unique from 0630. CVE ID : CVE	sts, aka IB Remote on '. This CVE ID n CVE-2019-	guidai visory 2019-	•		
N/A	05-03-2019	5.5	An information vulnerability Windows Hyphost operation to properly version an author on a guest operation and a guest operation with the system, aka 'Version and the system and	al.msr osoft.c	•	O-MIC WIND 04041		
N/A	05-03-2019	2.1	An information vulnerability Windows implication discloses file aka 'Windows' Disclosure Vulnerability CVE ID : CVE	al.msr osoft.c	•	O-MIC WIND 04041		
N/A	05-03-2019	4.3	An information vulnerability the Windows component in discloses the its memory, a GDI Informat Disclosure Vulnerability CVE-2019-06 2019-0615, C	al.msr osoft.c	•	O-MIC WIND 04041		
CV Scoring Scal (CVSS)	e 0-1 1-	2 2	1-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Publish Date	cvss	Description & CVE ID		Patch		NCII	NCIIPC ID	
		0616, CVE-2019-0619, CVE-2019-0664.						
05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663. CVE ID: CVE-2019-0661			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0661		O-MIC- WIND- 040419/518	
05-03-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0662		O-MIC- WIND- 040419/519	
05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID		https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0663		O-MIC- WIND- 040419/520		
			4-5	5-6	6-7	7-8	8-9	9-10
	05-03-2019 05-03-2019 0-1 1-e(s): CSRF- Cross Si	05-03-2019 9.3 05-03-2019 2.1 0-1 1-2 2 e(s): CSRF- Cross Site Reque	CVE-2019-0 CVE ID : CV An informa vulnerabilit the Window improperly objects in model of the way that the Graphics Described (GDI) handled is unique from the way that the Graphics Described (GDI) handled is unique from the way that the Graphics Described (GDI) handled is unique from the window improperly objects in model with the window improperly objects in model of the window improperly objects in mode	CVE-2019-0664. CVE ID: CVE-2019 An information disc vulnerability exists the Windows kerne improperly handles objects in memory, 'Windows Kernel Information Disclos Vulnerability'. This is unique from CVE-0621, CVE-2019-06 CVE ID: CVE-2019-06 CVE ID: CVE-2019-06 GVE ID: CVE-2019-06 CVE ID: CVE-2019-06 CVE ID: CVE-2019-06 CVE ID: CVE-2019 A remote code exect vulnerability exists way that the Windo Graphics Device Int (GDI) handles object the memory, aka 'GI Remote Code Execut Vulnerability'. This is unique from CVE-0618. CVE ID: CVE-2019 An information disc vulnerability exists the Windows kerne improperly initialize objects in memory.' exploit this vulneral an authenticated atticuld run a specially crafted application, 'Windows Kernel Information Disclos Vulnerability'. This O-1 1-2 2-3 3-4 4-5 e(s): CSRF- Cross Site Request Forgery; Dir. Trav Direction improperty in trav Direction in the content of	CVE ID: CVE-2019-0660 An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663. CVE ID: CVE-2019-0663. CVE ID: CVE-2019-0661 A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662 An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory.To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID O-1 1-2 2-3 3-4 4-5 5-6 e(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Trav.	CVE ID: CVE-2019-0660 An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663. CVE ID: CVE-2019-0661 A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662 An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID O-1 1-2 2-3 3-4 4-5 5-6 6-7 e(s): CSRF- Cross Site Request Forgery; Dir. Trav Directory Traversal; +Information Di	CVE-2019-0664. CVE ID: CVE-2019-0660 An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka "Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661. A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0661. CVE ID: CVE-2019-0661 A remote code execution vulnerability'. This CVE ID is unique from CVE-2019-0662. CVE ID: CVE-2019-0662 An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID D1 12 23 34 4-5 5-6 6-7 7-8	CVE-2019-0664. CVE ID: CVE-2019-0660 An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel liformation Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663. CVE ID: CVE-2019-0663. CVE ID: CVE-2019-0661 A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662 An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID information Disclosure Vulnerabi

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2019- 0621, CVE-2019-0661.		
			CVE ID : CVE-2019-0663		
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0664	O-MIC- WIND- 040419/521
			CVE ID : CVE-2019-0664		
N/A	12-03-2019	6.8	Untrusted search path vulnerability in Windows 7 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	N/A	O-MIC- WIND- 040419/522
			CVE ID : CVE-2019-5921		
windows_8.1					
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0595	O-MIC- WIND- 040419/523

 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)	Publis	h Dat	е	cvss		Descrip	tion & CV	E ID	Pa	itch	NCII	PC ID
N/A	05-03-	2019		9.3	A revuling the Englosis under the Code Vuling is under the Code CVE 201 062	emote conerability Window, sine implects in nabase Electron Execution of the Execution of t	ty'. This om CVE 2019-05 0598, CV , CVE-20	ution when tabase handles aka 'Jet mote CVE ID -2019- 97, 'E- 19-	al.msr osoft.c	•	O-MIC WIND 04041	
N/A	05-03-	2019		9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.				al.msr osoft.c	com/en ecurity- nce/ad e/CVE-	O-MIC WIND 04041	
N/A	05-03-	2019	,	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-		O-MIC WIND 04041	
CV Scoring Scale (CVSS) Vulnerability Typ	pe(s): CSR			Reque	_			5-6 ectory Trav			8-9	9-10 n; DoS-

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descrip	tion & CV	E ID	Pa	itch	NCI	IPC ID
					Vuli is un 059 CVE 201 062	nique fr 5, CVE- -2019- 9-0599 5.	ty'. This om CVE 2019-05 0597, CV , CVE-20	-2019- 96, Έ- 19-	2019-	0598		
N/A	05-	-03-201	9	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0625.				al.msr osoft.c	•	O-MIC WIND 04041	
N/A	05	-03-201	9	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601. CVE ID: CVE-2019-0600				al.msr osoft.c	,	O-MIC WIND 04041	
N/A	05	-03-201	9	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component				al.msr	//port c.micr com/en ecurity-	O-MIC WIND 04041	
CV Scoring Scale (CVSS)	e	0-1	1-2	2 2	!-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID				
					obj 'HI Dis Thi	ects in n D Inforn closure is CVE II E-2019-	Vulneral) is uniq	aka pility'. ue from	guidar visory 2019-	•						
N/A	05-	-03-201	9	4.3	vul the cor dis its GD Dis Thi CVI 202 063 CVI	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0602				//port c.micr com/en ecurity- nce/ad /CVE- 0602	O-MIC WIND 04041					
N/A	05-	-03-201	9	4.3	vul the cor dis its GD Dis Thi CVI 202 062 CVI	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0615				//port c.micr com/en ecurity- nce/ad /CVE- 0615	O-MIC WIND 04041					
N/A	05	-03-201	9	4.3	An information disclosure vulnerability exists when									//port c.micr	O-MIC WIND	
CV Scoring Scale (CVSS)	е	0-1	1-2	2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10				

Vulnerability Type(s)	Publish Date	cvss	Descripti	ion & CVE ID	Pa	atch	NCII	PC ID
			its memory, GDI Informa Disclosure V This CVE ID CVE-2019-0 2019-0615, 0619, CVE-2 CVE-2019-0	improperly e contents of aka 'Windowntion Vulnerability'. is unique from 602, CVE-CVE-2019-2019-0660,	-US/s guida visory 2019-	com/en ecurity- nce/ad y/CVE- -0616	04041	9/532
N/A	05-03-2019	9.3	A remote covulnerability way that the Graphics De (GDI) handle the memory Remote Cod Vulnerabilitis unique from 1662.	https://discrete.com/discrete.c	://port rc.micr com/en ecurity- nce/ad y/CVE- -0618	O-MIC WIND- 04041	-	
N/A	05-03-2019	4.3	An informativulnerability the Window component discloses the its memory, GDI Information Disclosure Varies CVE-2019-0 2019-0615, 0616, CVE-2019-0 CVE ID : CVE ID : CVE ID : CVE ID in the component of the compon	https: al.msi osoft. -US/s guida visory 2019-	://port rc.micr com/en ecurity- nce/ad y/CVE- -0619	O-MIC WIND- 04041	-	
CV Scoring Scale (CVSS)	e 0-1 1-	2 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	05-03-2019	2.1	'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019- 0661, CVE-2019-0663. -US/security- guidance/ad visory/CVE- 2019-0621	D-MIC- WIND- 040419/535
_			CVE ID : CVE-2019-0621	_
N/A	05-03-2019	7.2	properly handle objects in -US/security- W	D-MIC- VIND- 040419/536
N/A	05-03-2019	9.3	Vulnerability'. This CVE ID -US/security-	D-MIC- VIND- 040419/537
N/A	05-03-2019	7.5	vulnerability exists in the al msrc micr	D-MIC- VIND-
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 Da	te CVS	S	Descrip	tion & CV	E ID	Pa	itch	NCII	PC ID
			ser pac aka Ser Exc	vice who ds speci ckets to a 'Windo ver Rem ecution V	ally craf a DHCP s ws DHC lote Cod Vulnerab	ted server, p e ility'.	-	•	04041	.9/538
N/A	05-03-201	9 2.1	vul the imp ker 'Wi Dis	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628				//port c.micr com/en ecurity- nce/ad r/CVE- 0628	O-MIC WIND 04041	
N/A	05-03-201	9 9	vul wa Ser (SM cer 'Wi Coo Vul is u 063	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.				//port c.micr com/en ecurity- nce/ad /CVE- 0630	O-MIC WIND 04041	
N/A	05-03-201	9 9	A r vul wa Ser (SM cer 'Wi Coo	CVE ID: CVE-2019-0630 A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-			al.msr osoft.c	•	O-MIC WIND 04041	
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
			0630. CVE ID : CVE-2019-0633		
N/A	05-03-2019	5.5	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. CVE ID: CVE-2019-0635	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0635	O-MIC- WIND- 040419/542
N/A	05-03-2019	2.1	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'. CVE ID: CVE-2019-0636	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0636	O-MIC- WIND- 040419/543
N/A	05-03-2019	6.9	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0656	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0656	O-MIC- WIND- 040419/544
N/A	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.		https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0660	O-MIC- WIND- 040419/545	

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	itch	NCII	PC ID
					CVI 201 061 CVI	s CVE ID E-2019-0 19-0615 16, CVE-2	0602, CV , CVE-20 2019-06 0664.	Έ- 19- 19,				
						E ID : CV						
N/A	05	-03-201	9	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618.				al.msr osoft.c	•	O-MIC WIND 04041	
					CVI	E ID : CV	E-2019	-0662				
N/A	05	-03-201	9	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661. CVE ID: CVE-2019-0663				al.msr osoft.c	•	O-MIC WIND 04041	
N/A	05	-03-201	9	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of				al.msr osoft.c	//port c.micr com/en ecurity- nce/ad		
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty		: CSRF- Cronial of Serv		_				_			ntormatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Descript	tion & CVE ID)	Pa	tch	NCII	PC ID
			its memory GDI Inform Disclosure This CVE ID CVE-2019-0 2019-0615 0616, CVE-2 CVE-2019-0	ation Vulnerabilit Dis unique f D602, CVE- , CVE-2019 2019-0619, D660.	ty'. From	visory 2019-0			
windows_rt_8	3.1				L				
N/A	05-03-2019	9.3	A remote convulnerability the Window Engine impospects in modulate Engine Execution of the Windows Engine in modulate Engine Execution of the Winerability Engine Execution of the Winerability Engine Execution of the Winerability Execution of the	ty exists who is Jet Datab roperly har nemory, akangine Remo tion ty'. This CVI om CVE-20 2019-0597, 0598, CVE-	en dase idles i 'Jet ote E ID		c.micr om/en ecurity- ace/ad /CVE-	O-MIC WIND 04041	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.		on en ease adles a 'Jet ote E ID		c.micr om/en ecurity- ace/ad /CVE-	O-MIC WIND 04041	
CV Scoring Scal (CVSS)	e 0-1 1:		2-3 3-4		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-2019-0596		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0597	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0597	O-MIC- WIND- 040419/551
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0598	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0598	O-MIC- WIND- 040419/552
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0599	O-MIC- WIND- 040419/553

Vulnerability Type(s)	Publish Date	cvss	Description &	CVE ID	Pa	tch	NCII	PC ID
			is unique from C 0595, CVE-2019-0597, CVE-2019-0598, CVE-0625.	·0596, CVE- ·2019-				
N/A	05-03-2019	1.9	An information of vulnerability exist the Human Interduces (HID) comproperly hand objects in memory 'HID Information Disclosure Vulnerability CVE-2019-0601.	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041		
N/A	05-03-2019	1.9	An information of vulnerability exist the Human Interduces (HID) comproperly hand objects in memory 'HID Information Disclosure Vulnerability CVE-2019-0600. CVE ID: CVE-20	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041		
N/A	05-03-2019	4.3	An information of vulnerability exist the Windows GD component imprediscloses the consist memory, aka GDI Information Disclosure Vulnerability CVE ID is un	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041		
CV Scoring Scale (CVSS)	e 0-1 1-	2 2	-3 3-4 4-5	_	6-7	7-8	8-9	9-10

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	atch	NCII	PC ID
					201 061 CVI	19-0616 19, CVE- E-2019-0	0615, CV , CVE-20 2019-06 0664. (E-2019	19- 60,				
N/A	05	-03-201	9	4.3	vulthe condiscondi	merability Windown ponenty closes the memory I Inform closure S CVE ID E-2019-0 19-0616 19, CVE-1	imprope conter , aka 'Wi ation Vulneral is uniqu 0602, CV CVE-20	when erly nts of ndows bility'. ue from E- 19- 60,	al.msr osoft.c -US/so guidan	//port rc.micr com/en ecurity- nce/ad r/CVE- 0615	O-MIC WIND 04041	
N/A	05	-03-201	9	4.3	vulthe condiscondi	merability Windown ponent closes the memory I Inform closure S CVE ID E-2019-0 19-0615 19, CVE-1	imprope conter , aka 'Wi ation Vulneral is uniqu 0602, CV CVE-20	when erly nts of indows bility'. ue from E- 19- 60,	al.msr osoft.c -US/so guidan	//port c.micr com/en ecurity- nce/ad r/CVE- 0616	O-MIC WIND 04041	
N/A	05	-03-201	9	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface https://p				com/en	O-MIC WIND 04041		
CV Scoring Scale (CVSS) O-1 1-2 2-3 Vulnerability Type(s): CSRF- Cross Site Request				2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	

Type(s)	Publis	h Date	C	VSS		Descrip	tion & CV	E ID	Pa	itch	NCII	PC ID
					the Ren Vuli is u 066	memor note Coo nerabili nique fr 12.	les objec y, aka 'G de Execu ty'. This om CVE 'E-2019	DI+ ition CVE ID -2019-	_	nce/ad /CVE- 0618		
N/A	05-03-	2019	4.	3	vuli the com disc its r GDI Disc This CVE 201 061 CVE	merability Windown ponent closes the memory Inform closure is CVE IE C-2019-6, CVE-C-2019-6	improp le conter , aka 'W' ation Vulneral) is uniqu 0602, CV , CVE-20	when erly nts of indows bility'. ue from E- 19- 60,	al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad r/CVE- 0619	O-MIC WIND 04041	
N/A	05-03-	2019	2.	.1	vuli the imp obje 'Wii Info Vuli is u 066	nerability Window Properly Pects in notion Indows Internation Inte	tion disc ty exists vs kerne handles nemory, Kernel n Disclos ty'. This om CVE 2019-06	when l aka sure CVE ID -2019-	al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad r/CVE- 0621	O-MIC WIND 04041	
N/A	05-03-	2019	7.	2	Windows when the osoft.com/en W				O-MIC WIND 04041			
CV Scoring Scale (CVSS)	U	-1	1-2		-3	3-4	4-5	5-6	6-7	7-8 fo- Gain Ir	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			memory, aka 'Win32k Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0623	visory/CVE- 2019-0623	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599. CVE ID: CVE-2019-0625	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0625	O-MIC- WIND- 040419/563
N/A	05-03-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. CVE ID: CVE-2019-0626	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0626	O-MIC- WIND- 040419/564
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0628	O-MIC- WIND- 040419/565

Vulnerability Type(s)	Pub	lish Da	te	cvss		Descript	tion & CV	E ID	Pa	itch	NCI	IPC ID
N/A	05-0	3-201	9	9	vulr way Serv (SM cert 'Win Cod Vuln is un 063	nerability that the ver Mes Bv2) set ain requal to Execusing the Execusion E	ty'. This om CVE	in the soft ck 2.0 ndles ca note CVE ID -2019-	al.msr osoft.c	-	O-MIC WIND 04041	
					CVE	ID : CV	E-2019	-0630				
N/A	05-0	3-201	9	9	vulr way Serv (SM cert 'Wir Cod Vulr is ur 063	nerability that the ver Mes Bv2) se ain requal to Execusing the contraction of the contra	ode execty exists e Microssage Blowrver har uests, ake tion ty'. This om CVE	in the soft ck 2.0 ndles ca note CVE ID -2019-	al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad r/CVE- 0633	O-MIC WIND 04041	
N/A	05-0	3-201	9	2.1	vulr Win disc aka Disc	dows in loses fil 'Windo closure	tion ty exists nproper le inforn ws Infor Vulneral	ly nation, mation bility'.	al.msr osoft.c -US/se guidan visory	/CVE-	O-MIC WIND 04041)-
N/A	05-0	3-201	9	6.9	vulr the to p in m	nerabili Windov roperly nemory,	n of priv ty exists vs kerne handle aka 'Wi	when I fails objects ndows	guidance/ad visory/CVE- 2019-0636 https://port al.msrc.micr osoft.com/en -US/security-guidance/ad visory/CVE- guidance/ad 040419/5)-
CV Scoring Scale (CVSS)	9	0-1	1-2	2 2	!-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
()								ectory Trav				

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID
			Privilege V	ılnerabi	lity'.	2019-	0656		
			CVE ID : CV	E-2019	-0656				
N/A	05-03-2019	4.3	CVE-2019- 2019-0615 0616, CVE- CVE-2019-	ty exists vs GDI improp le conter , aka 'Wi ation Vulneral 0 is uniqu 0602, CV , CVE-20 2019-06	when erly ats of andows bility'. ue from E- 19-	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
N/A	05-03-2019	9.3	This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0664. CVE ID: CVE-2019-0660 A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662 An information disclosure vulnerability exists when			-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
N/A	05-03-2019	2.1		-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041			
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross Denial of Service	_		Sql- SQL Ir	_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019- 0621, CVE-2019-0661.		
			CVE ID : CVE-2019-0663		
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0664	O-MIC- WIND- 040419/573
windows_serv	ver_2008				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0595	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0595	O-MIC- WIND- 040419/574
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when	https://port al.msrc.micr	O-MIC- WIND-

CV Scoring Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
(CV33)										

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019- 0595, CVE-2019-0597, CVE-2019-0598, CVE- 2019-0599, CVE-2019- 0625. CVE ID: CVE-2019-0596	osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0596	040419/575
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0597	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0597	O-MIC- WIND- 040419/576
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0598	O-MIC- WIND- 040419/577

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			2019-0599, CVE-2019- 0625. CVE ID : CVE-2019-0598		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625.	https://post	O-MIC- WIND- 040419/578
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601. CVE ID: CVE-2019-0600	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0600	O-MIC- WIND- 040419/579
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0601	O-MIC- WIND- 040419/580
CV Scoring Scale	e 0-1 1	-2 2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Vulnerability Type(s)	P	ublish Da	ate	CVSS		Descript	tion & CV	E ID	Pa	tch	NCII	PC ID
					CVI	E-2019-(0600.					
					CVI	E ID : CV	E-2019	-0601				
N/A	05	-03-201	9	4.3	vuli the con disc its i GDI Disc Thi CVI 201 061 CVI	merability Windown ponenty closes the memory I Inform closure S CVE ID E-2019-0 19, CVE-1 E-2019-0	improp le conter , aka 'Wi ation Vulneral) is uniqu 0615, CV , CVE-20 2019-06	when erly nts of indows bility'. ue from E- 19- 60,	al.msr osoft.c -US/se guidar	//port c.micr com/en ecurity- nce/ad /CVE- 0602	O-MIC WIND 04041	
N/A	05	-03-201	9	4.3	An vuli the con disc its i GDI Disc Thi CVI 201 CVI	informa nerability Windown nponenty closes the memory I Inform closure S CVE ID E-2019-0 E-2019-0 E ID : CVE	tion disc cy exists vs GDI improp ee conter , aka 'Wi ation Vulneral 0 is uniqu 0602, CV 2019-06 2019-06	closure when erly of the soft indows oility'. Le from E-19-60,	al.msr osoft.c	,	O-MIC WIND 04041	
N/A	05	-03-201	9	4.3	tic /conviter							
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				_			Sql- SQL Ir	ctory Trav ijection; N			irormatic	on; DOS-

Vulnerability Type(s)	Publ	ish Da	te	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
					This CVE 201 061 CVE	s CVE IC -2019-(9-0615 9, CVE- -2019-(Vulneral) is uniqu)602, CV , CVE-20 2019-06)664. (E-2019	ue from E- 19- 60,	2019-	0616		
N/A	05-03	3-2019	9	9.3	vuli way Gra (GD the Ren Vuli is u	nerability that the phics Do I) hand memory note Coonerability in 12.	ode execty exists e Windo evice Intelles objecty, aka 'G', aka 'G', akg'. This om CVE	in the ws erface ts in DI+ tion CVE ID -2019-	al.msr osoft.c	•	O-MIC WIND 04041	
N/A	05-03	3-2019	9	4.3	vuli the com disc its r GDI Disc This CVE 201 061 CVE	merability Windown ponent closes the memory Inform closure is CVE ID 2-2019-0 15-2019-	impropage contertains, aka 'Winerale valuerale	when erly ats of andows bility'. ue from E- 19- 60,	al.msr osoft.c	com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
N/A	05-03	3-2019	9	2.1	vuli the imp	nerabilit Windov properly	tion disc ty exists vs kerne handles nemory,	when l	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad			-
CV Scoring Scale (CVSS)	e	0-1	1-2	2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Da	ate CVS		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
			Info Vul is u	indows I ormation Inerabili unique fr 61, CVE-	n Disclos ty'. This om CVE	CVE ID -2019-	visory 2019-	-		
			CV.	E ID : CV	E-2019	-0621				
N/A	05-03-201	.9 7.2	vul Wi Wi pro me Ele Vul	operly ha mory, ak vation o Inerabili	y exists when the apponent of the control of the co	in t fails to jects in 2k ge	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
N/A	05-03-201	9 9.3	A r vul the Eng obj Dat Coo Vul is u 05% CV2 20%	Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0623 A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599. CVE ID: CVE-2019-0625 A memory corruption				//port c.micr com/en ecurity- nce/ad /CVE- 0625	O-MIC WIND 04041	
N/A	05-03-201	7.5	vul Wi ser ser pad aka	CVE ID: CVE-2019-0625 A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code				//port c.micr com/en ecurity- nce/ad /CVE- 0626	O-MIC WIND 04041	
CV Scoring Scal (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cr Denial of Ser	_				_			nformatio	n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Execution Vulnerability'.		
			CVE ID : CVE-2019-0626		
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0628	O-MIC- WIND- 040419/590
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0630	O-MIC- WIND- 040419/591
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630. CVE ID: CVE-2019-0633	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0633	O-MIC- WIND- 040419/592
N/A	05-03-2019	5.5	An information disclosure	https://port	O-MIC-

Vulnerability Type(s)	P	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID									
					hos to p from on a syst Hyp Disc	ndows Het operate or operly man auto a guest of tem, aka per-V Infoliosure of the tem of t	ing syste validate henticat operating 'Windo formatio Vulneral	em fails e input ed user g ws n pility'.	-US/se	•	04041	9/593									
N/A	05	-03-201	9	2.1	vuli Wir disc aka Disc	informa nerabilit ndows ir closes fil 'Windo closure' E ID : CV	y exists nproper e inform ws Infor Vulneral	ly nation, mation pility'.	al.msr osoft.c	•	O-MIC WIND 04041										
N/A	05	-03-201	9	4.3	vuli the con disc its i GDI Disc Thi CVI 201 061 CVI	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0619, CVE-2019-0664. CVE ID: CVE-2019-0660				//port c.micr com/en ecurity- nce/ad /CVE- 0660	O-MIC WIND 04041										
N/A	05	-03-201	9	2.1	vuli the imp obje 'Wi	informa nerabilit Windov oroperly ects in n ndows I	y exists vs kerne handles nemory, Kernel	when l aka	al.msr osoft.c	//port c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041										
CV Scoring Scale (CVSS)		0-1	1-2		2-3 st For	3-4	4-5	5-6	6-7 ersal: +In	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	Descr	ption & CV	E ID	Pa	tch	NCII	PC ID		
			Vulnerab is unique 0621, CVI	from CVE	-2019-	2019-	0661				
			CVE ID : (CVE-2019	-0661						
N/A	05-03-2019	9.3	the memore Control Remote Control Vulnerabilis unique 0618.	lity exists the Windo Device Int dles objec ory, aka 'G ode Execu ility'. This from CVE	in the ows erface ets in DI+ etion CVE ID -2019-	-US/se	c.micr com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041			
			CVE ID : (CVE-2019	-0662						
N/A	05-03-2019	2.1	vulnerabithe Windimproper objects in exploit that an auther could runcrafted ap 'Windows Informativulnerabits unique 0621, CVI	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661.				O-MIC WIND 04041			
N/A	05-03-2019	4.3	An inform vulnerabi the Wind- compone discloses its memo GDI Infor	lity exists ows GDI nt improp the conter ry, aka 'W	-US/se	c.micr com/en ecurity- nce/ad	O-MIC WIND 04041				
CV Scoring Scal (CVSS)	0-1		2-3 3-4	4-5	5-6	6-7	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	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0660.	2019-0664	
			CVE ID : CVE-2019-0664		
windows_serv	ver_2012				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0595	O-MIC- WIND- 040419/600
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0596	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0596	O-MIC- WIND- 040419/601

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0597	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0597	O-MIC- WIND- 040419/602
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0598	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0598	O-MIC- WIND- 040419/603
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0599	O-MIC- WIND- 040419/604

 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
			0595, CVE-2019-0596, CVE-2019-0597, CVE- 2019-0598, CVE-2019- 0625. CVE ID : CVE-2019-05		
N/A	05-03-2019	1.9	An information disclosivulnerability exists who the Human Interface Devices (HID) componed improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability This CVE ID is unique from CVE-2019-0601. CVE ID: CVE-2019-0601	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0600	O-MIC- WIND- 040419/605
N/A	05-03-2019	1.9	An information disclosivulnerability exists who the Human Interface Devices (HID) componed improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability This CVE ID is unique from CVE-2019-0600.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0601	O-MIC- WIND- 040419/606
N/A	05-03-2019	4.3	An information disclose vulnerability exists who the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability This CVE ID is unique for CVE-2019-0615, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0602	O-MIC- WIND- 040419/607
CV Scoring Scal	e 0-1 1	-2 2	3-4 4-5 5	-6 6-7 7-8	8-9 9-10

Vulnerability Type(s)	Р	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID	
					061 CVI	9, CVE- E-2019-0	, CVE-20 2019-06 0664. ' E-2019	60,					
N/A	05	-03-201	9	4.3	vult the con disc its i GDI Disc Thi CVI 201 061 CVI	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0615				//port c.micr com/en ecurity- nce/ad /CVE- 0615	O-MIC WIND 04041		
N/A	05	-03-201	9	4.3	the con discourse of the condition of th	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0616				//port c.micr com/en ecurity- nce/ad /CVE- 0616	O-MIC WIND 04041		
N/A	05	-03-201	9	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad		0-MIC WIND 04041		
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	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; SqI- SQL Injection; N/A- Not Applicable.										

Vulnerability Type(s)	Pi	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID
					Ren Vul is u 066	note Coonerabili nique fr 52.	y, aka 'G de Execu ty'. This om CVE	tion CVE ID -2019-	visory 2019-	-		
N/A	05-	-03-201	9	4.3	vult the con disc its i GDI Disc Thi CVI 201 061 CVI	merability Windown ponent closes the memory Inform closure s CVE ID E-2019-0 19-0615 6, CVE-1	impropo e conter , aka 'Wi ation Vulneral) is uniqu 0602, CV , CVE-20 2019-06	when erly ats of ndows bility'. ae from E- 19- 60,	https://port of al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0619			- - 9/611
N/A	05-	-03-201	9	2.1	vuli the imp obje 'Wi Info Vul is u 066	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663. CVE ID: CVE-2019-0621				//port c.micr com/en ecurity- nce/ad /CVE- 0621	O-MIC WIND 04041	
N/A	05-	-03-201	9	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k				al.msr osoft.c	com/en ecurity- nce/ad	O-MIC WIND 04041	
CV Scoring Scale (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7 ersal; +In	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Descrip	tion & CV	E ID	Pa	tch	NCII	PC ID										
			Elevation o Vulnerabili		ge	2019-	0623												
			CVE ID : CV	E-2019	-0623														
N/A	05-03-2019	9.3	A remote covulnerabilithe Window Engine impobjects in notabase Engine Execution of the Exec	al.msr osoft.c -US/se guidar	com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041													
N/A	05-03-2019	7.5	A memory vulnerability Windows S service who sends specipackets to a aka 'Windo Server Rem	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.				O-MIC WIND 04041											
N/A	05-03-2019 05-03-2019	2.1	An information vulnerability the win32k improperly kernel information with the win32k In Disclosure CVE ID : CV	al.msr osoft.c -US/se guidan visory 2019-	•	O-MIC WIND 04041	- .9/616												
CV Scoring Scal	e 0-1	1-2 2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10										
(CVSS) Vulnerability Ty																			
	Denial of Service	e; XSS- Cross	Site Scripting;		ijection; N	/A- Not A	pplicable.		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)	P	ublish Da	ate	cvss		Descript	tion & CV	E ID	Pa	tch	NCI	IPC ID
					way Serv (SM cert 'Win Cod Vuln is un 063	that the ver Messain required Execuning the Execution the	ey exists e Micros sage Blo rver har uests, ak SMB Ren tion ty'. This om CVE	soft ck 2.0 ndles a note CVE ID -2019-	osoft.c	-	WIND 04041	19/617
N/A	05	-03-201	9	9	vulr way Serv (SM cert 'Wir Cod Vulr is ur 063	nerability that the ver Mes. Bv2) see ain requested Execunique from 0.	ode exectly exists age Bloor rver har uests, ake tion ty'. This om CVE	in the soft ck 2.0 ndles ca note CVE ID -2019-	al.msr osoft.c		O-MIC WIND 04041	
N/A	05	-03-201	9	5.5	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. CVE ID: CVE-2019-0635				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0635		O-MIC WIND 04041	
N/A	05	-03-201	.9	2.1	An i	nforma nerabilit		when	al.msr	//port c.micr com/en	O-MIC WIND	
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty				_			Sql- SQL Ir	ectory Trav njection; N			nformatio	on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			discloses file information, aka 'Windows Information Disclosure Vulnerability'. CVE ID: CVE-2019-0636	-US/security- guidance/ad visory/CVE- 2019-0636	040419/620
N/A	05-03-2019	6.9	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0656	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0656	O-MIC- WIND- 040419/621
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0664. CVE ID: CVE-2019-0660	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0660	O-MIC- WIND- 040419/622
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0661	O-MIC- WIND- 040419/623

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0661		
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0662	O-MIC- WIND- 040419/624
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661. CVE ID: CVE-2019-0663	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0663	O-MIC- WIND- 040419/625
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0664	O-MIC- WIND- 040419/626

 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	
			2019-0615, CVE-2019- 0616, CVE-2019-0619, CVE-2019-0660.						
	2016		CVE ID : CVE-2019-0664						
windows_ser	ver_2016		A romoto a	o do ovog	ıtion				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0595			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0595		O-MIC- WIND- 040419/627	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0596			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0596		O-MIC- WIND- 040419/628	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database			https://port al.msrc.micr osoft.com/en		O-MIC- WIND- 040419/629	
CV Scoring Scal (CVSS)	e 0-1 1-	2 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
			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0597	-US/security- guidance/ad visory/CVE- 2019-0597	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0598	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0598	O-MIC- WIND- 040419/630
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0598, CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0599	O-MIC- WIND- 040419/631

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			0625. CVE ID : CVE-2019-0599		
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601. CVE ID: CVE-2019-0600	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0600	O-MIC- WIND- 040419/632
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600. CVE ID: CVE-2019-0601	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0601	O-MIC- WIND- 040419/633
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0615, CVE-2019-0616, CVE-2019-0660,	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0602	O-MIC- WIND- 040419/634

Vulnerability Type(s)	Р	ublish Da	ite	cvss		Descript	ion & CV	E ID	Pa	itch	NCII	PC ID
					CVE	E-2019-(0664.					
					CVI	E ID : CV	E-2019	-0602				
N/A	N/A 05-03-2		05-03-2019 4.3			vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0615 An information disclosure				//port c.micr com/en ecurity- nce/ad //CVE- 0615	O-MIC WIND 04041	
N/A	05	-03-201	9	4.3				al.msr osoft.c	•	O-MIC WIND 04041		
N/A	05	-03-201	9	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-		O-MIC WIND 04041	
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 Ty		ial of Serv		_			Sql- SQL In	_			normatio	iii; D05-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0662. CVE ID: CVE-2019-0618	2019-0618	
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0619	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0619	O-MIC- WIND- 040419/638
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663. CVE ID: CVE-2019-0621	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0621	O-MIC- WIND- 040419/639
N/A	05-03-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0623	O-MIC- WIND- 040419/640

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			Vulnerability'. CVE ID: CVE-2019-0623			
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599. CVE ID: CVE-2019-0625	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0625	O-MIC- WIND- 040419/641	
N/A	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'.		vulnerability exists in the Windows Server DHCP service when an attacker sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0626	O-MIC- WIND- 040419/642	
			A security feature bypass			
N/A	05-03-2019 4.6		vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-2019-0632.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0627	O-MIC- WIND- 040419/643	

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0627		
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628 A remote code execution https://p al.msrc.m osoft.com -US/secu guidance visory/CV 2019-062		O-MIC- WIND- 040419/644
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633. CVE ID: CVE-2019-0630	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0630	O-MIC- WIND- 040419/645
N/A	05-03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0632. CVE ID: CVE-2019-0631	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0631	O-MIC- WIND- 040419/646
N/A	05-03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to	https://port al.msrc.micr osoft.com/en -US/security-	O-MIC- WIND- 040419/647

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE- 2019-0631.	guidance/ad visory/CVE- 2019-0632	
			CVE ID : CVE-2019-0632		
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0633	O-MIC- WIND- 040419/648
N/A	05-03-2019	5.5	An information disclosure vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. CVE ID: CVE-2019-0635	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0635	O-MIC- WIND- 040419/649
N/A	05-03-2019	2.1	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-	O-MIC- WIND- 040419/650

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID	
			CVE ID : CVE-2019-0636	2019-0636		
N/A	05-03-2019	5	A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections, aka 'Windows Defender Firewall Security Feature Bypass Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0637	O-MIC- WIND- 040419/651	
			CVE ID: CVE-2019-0637			
N/A	05-03-2019	6.9	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0656	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0656	O-MIC- WIND- 040419/652	
N/A	05-03-2019	4.4	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0659	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0659	O-MIC- WIND- 040419/653	
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0660	O-MIC- WIND- 040419/654	

Vulnerability Type(s)	Publish D	ate	cvss		Descript	tion & CV	E ID	Pa	tch	NCII	PC ID
				CVE 201 061	2019-0 9-0615) is uniq 0602, CV , CVE-20 2019-06 0664.	⁄Е-)19-				
				CVI	E ID : CV	E-2019	-0660				
N/A	05-03-203	19	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662				al.msr osoft.c -US/se guidar	com/en ecurity- nce/ad r/CVE-	O-MIC WIND 04041	
				CVE	E ID : CV	E-2019	-0662				
N/A	05-03-203	19	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes objects in memory. To exploit this vulnerability, an authenticated attacker could run a specially crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0661. CVE ID: CVE-2019-0663			al.msr osoft.c	•	O-MIC WIND 04041		
windows_serv	ver_2019									1	
N/A	05-03-201	19	9.3	vulı	A remote code execution vulnerability exists when the Windows Jet Database			https://port al.msrc.micr osoft.com/en		0-MIC WIND 04041	
CV Scoring Scale	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
			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0596, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0595	-US/security- guidance/ad visory/CVE- 2019-0595	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0596	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0596	O-MIC- WIND- 040419/658
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0599, CVE-2019-	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0597	O-MIC- WIND- 040419/659

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCII	PC ID
			0625. CVE ID : CV	E-2019-()597				
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0599, CVE-2019-0625. CVE ID: CVE-2019-0598 A remote code execution			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0598 e es et https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0599		O-MIC WIND 04041	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625. CVE ID: CVE-2019-0599		O-MIC- WIND- 040419/661				
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component improperly handles objects in memory, aka 'HID Information			https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-		I WIIND-	
CV Scoring Scal (CVSS)	e 0-1 1-		2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Publish Date	cvss	Description	n & CVE ID	Pa	tch	NCII	PC ID
			Disclosure Vu This CVE ID is CVE-2019-060	unique from	2019-0	0600		
			CVE ID : CVE-	2019-0600				
N/A	05-03-2019 1.9 vu the De im ob 'H! Dis Th		the Human Into Devices (HID) improperly had objects in mer 'HID Informat Disclosure Vu	lity exists when in Interface HID) component ly handles memory, akarmation e Vulnerability'.		//port c.micr om/en ecurity- ace/ad /CVE- 0601	O-MIC- WIND- 040419/663	
			CVE ID : CVE-	2019-0601				
N/A	05-03-2019	4.3	An information vulnerability of the Windows component implication discloses the control of the component implication of the componen	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0602		O-MIC WIND 04041		
N/A	05-03-2019	4.3	An information vulnerability of the Windows component im discloses the control of the work	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0615		O-MIC- WIND- 040419/665		
CV Scoring Scale	e 0-1 1-	-2 2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Vulnerability Type(s)	Pι	ıblish Da	ite	cvss		Descript	ion & CV	E ID	Pa	tch	NCII	PC ID	
					CVI 201 061 CVI	s CVE IC E-2019-(19-0616 19, CVE- E-2019-(E ID : CV	0602, CV , CVE-20 2019-06 0664.	E- 19- 60,					
N/A	05-	03-201	9	4.3	vul the con disc its i GD Dis Thi CVI 203 061 CVI	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0616			al.msr osoft.c	•	O-MIC WIND 04041		
N/A	05-	03-201	9	9.3	vul way Gra (GI the Ren Vul is u 066	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0662. CVE ID: CVE-2019-0618			al.msr osoft.c	com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041		
N/A	05-	03-201	9	4.3	vul the con dise	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of its memory, aka 'Windows				https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE-		O-MIC- WIND- 040419/668	
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-									9-10				

Vulnerability Type(s)	Publish Date	cvss	Descript	ion & CVE	ID	Pa	tch	NCII	PC ID
			GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE- 2019-0615, CVE-2019- 0616, CVE-2019-0660, CVE-2019-0664. CVE ID: CVE-2019-0619 An information disclosure			2019-	0619		
N/A	05-03-2019	2.1	An informate vulnerability the Windows improperly objects in moderability with the Windows K of the Windows	y exists was kernel handles lemory, a cernel Disclosury'. This Com CVE-22019-066	when ka tre VE ID 2019- 3.	al.msr osoft.c	com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041	
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0599. CVE ID: CVE-2019-0625		al.msr osoft.c -US/se	com/en ecurity- nce/ad /CVE-	O-MIC WIND 04041		
N/A	05-03-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker			https://port al.msrc.micr osoft.com/en -US/security-		O-MIC WIND 04041	
CV Scoring Scale (CVSS)	e 0-1 1-		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
			sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. CVE ID: CVE-2019-0626	guidance/ad visory/CVE- 2019-0626	
N/A	05-03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0631, CVE-2019-0632. CVE ID: CVE-2019-0627	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0627	O-MIC- WIND- 040419/672
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. CVE ID: CVE-2019-0628	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0628	O-MIC- WIND- 040419/673
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0633.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0630	O-MIC- WIND- 040419/674

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0630		
N/A	allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from		https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0631	O-MIC- WIND- 040419/675	
			CVE ID : CVE-2019-0631		
N/A	05-03-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0631.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0632	O-MIC- WIND- 040419/676
			CVE ID : CVE-2019-0632		
N/A	05-03-2019	9	A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 2.0 (SMBv2) server handles certain requests, aka 'Windows SMB Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0630. CVE ID: CVE-2019-0633	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0633	O-MIC- WIND- 040419/677
N/A	05-03-2019	5.5	An information disclosure	https://port	O-MIC-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists when Windows Hyper-V on a host operating system fails to properly validate input from an authenticated user on a guest operating system, aka 'Windows Hyper-V Information Disclosure Vulnerability'. CVE ID: CVE-2019-0635	al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0635	WIND- 040419/678
N/A	05-03-2019	2.1	An information vulnerability exists when Windows improperly discloses file information, aka 'Windows Information Disclosure Vulnerability'. CVE ID: CVE-2019-0636	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0636	O-MIC- WIND- 040419/679
N/A	05-03-2019	5	A security feature bypass vulnerability exists when Windows Defender Firewall incorrectly applies firewall profiles to cellular network connections, aka 'Windows Defender Firewall Security Feature Bypass Vulnerability'. CVE ID: CVE-2019-0637	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0637	O-MIC- WIND- 040419/680
N/A	05-03-2019	6.9	An elevation of privilege vulnerability exists when the Windows kernel fails to properly handle objects in memory, aka 'Windows Kernel Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0656	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0656	O-MIC- WIND- 040419/681

N/A 05-03-2	019 4.4	An elevation of privilege vulnerability exists when the Storage Service improperly handles file operations, aka 'Windows Storage Service Elevation of Privilege Vulnerability'. CVE ID: CVE-2019-0659 An information disclosure vulnerability exists when	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0659	O-MIC- WIND- 040419/682
N/A 05-03-2	019 4.3	the Windows GDI component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0664.	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0660	O-MIC- WIND- 040419/683
N/A 05-03-2	019 9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0618. CVE ID: CVE-2019-0662	https://port al.msrc.micr osoft.com/en -US/security- guidance/ad visory/CVE- 2019-0662	O-MIC- WIND- 040419/684
Motorola				
c1_firmware	010		NI / A	
N/A 07-03-2	019 10	An issue was discovered	N/A	O-MOT-C1_F-
CV Scoring Scale (CVSS)		2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
		est Forgery; Dir. Trav Directory Trav ss Site Scripting; Sql- SQL Injection; N, 270		ntormation; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNetworkTomographySe ttings API function, as demonstrated by shell metacharacters in the tomography_ping_number field. CVE ID: CVE-2019-9117		040419/685
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST	N/A	O-MOT-C1_F- 040419/686

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNTPServerSettings API function, as demonstrated by shell metacharacters in the system_time_timezone field. CVE ID: CVE-2019-9118		
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteSettings API function, as demonstrated by shell metacharacters in the staticroute_list field. CVE ID: CVE-2019-9119	N/A	O-MOT-C1_F- 040419/687
N/A	07-03-2019	10	An issue was discovered	N/A	O-MOT-C1_F-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetWLanACLSettings API function, as demonstrated by shell metacharacters in the wl(0).(0)_maclist field. CVE ID: CVE-2019-9120		040419/688
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function	N/A	O-MOT-C1_F- 040419/689

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			triggers a call to the system function with untrusted input from the request body for the SetSmartQoSSettings API function, as demonstrated by shell metacharacters in the smartqos_priority_devices field. CVE ID: CVE-2019-9121		
m2_firmware					
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetNetworkTomographySe ttings API function, as demonstrated by shell metacharacters in the tomography_ping_number field.	N/A	O-MOT- M2_F- 040419/690

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

Type(s)	Publish Date	CVSS	·			Pa	tch	NCI	IPC ID
			CVE ID : CV	E-2019	-9117				
N/A	07-03-2019	10	An issue was on Motorol devices with 1.01 and 1.1. This issue is Injection all remote attains arbitrary control of the Injection was allows attained arbitrary O via a crafted request. The any HNAP attriggers a consystem function, as by shell me the system field. CVE ID: CVE ID: CVE	N/A		O-MO M2_F- 04041			
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands			N/A		O-MO M2_F- 04041	
CV Scoring Scale (CVSS)	0-1 coe(s): CSRF- Cross S		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
			via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetStaticRouteSettings API function, as demonstrated by shell metacharacters in the staticroute_list field. CVE ID: CVE-2019-9119		
N/A	07-03-2019	10	An issue was discovered on Motorola C1 and M2 devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetWLanACLSettings API function, as demonstrated by shell metacharacters in the wl(0).(0)_maclist field. CVE ID: CVE-2019-9120	N/A	O-MOT- M2_F- 040419/693
N/A	07-03-2019	10	An issue was discovered	N/A	O-MOT-

Vulnerability Type(s)	Pub	lish Da	ite	cvss		Descript	ion & CV	E ID	Pa	atch	NCII	IPC ID
					1.01 This Inje rem arbi roo Inje allo arbi via a requ any trig syst untr requ by s the sma field	devices with firmware 1.01 and 1.07 respectively. This issue is a Command Injection allowing a remote attacker to execute arbitrary code, and get a root shell. A command Injection vulnerability allows attackers to execute arbitrary OS commands via a crafted /HNAP1 POST request. This occurs when any HNAP API function triggers a call to the system function with untrusted input from the request body for the SetSmartQoSSettings API function, as demonstrated by shell metacharacters in the smartqos_priority_devices field. CVE ID: CVE-2019-9121					M2_F- 04041	9/694
Moxa												
eds-405a_firm	nware)										
N/A	05-0	3-201	9	5	plai whi info	Moxa IKS and EDS store plaintext passwords, which may allow sensitive information to be read by someone with access to the device.		N/A			X-EDS 19/695	
N/A	05-0	3-201	9	5	Mox not	ka IKS ai properl	E-2019 nd EDS o y check n server	loes	N/A			X-EDS 19/696
CV Scoring Scal (CVSS)		0-1	1-2		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty								ectory Trav njection; N				n; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			which results in a readonly user being able to perform arbitrary configuration changes.		
			CVE ID : CVE-2019-6520		
N/A	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot. CVE ID: CVE-2019-6522 Moxa IKS and EDS do not implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack. CVE ID: CVE-2019-6524 Several buffer overflow vulnerabilities have been identified in Moxa IKS and		N/A	O-MOX-EDS 040419/697	
N/A			implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack.	N/A	O-MOX-EDS 040419/698
N/A			N/A	O-MOX-EDS 040419/699	
N/A	05-03-2019	4	Moxa IKS and EDS allow remote authenticated users to cause a denial of service via a specially crafted packet, which may	N/A	O-MOX-EDS 040419/700

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			cause the switch to crash.		
			CVE ID : CVE-2019-6559		
N/A	05-03-2019	6.8	Cross-site request forgery has been identified in Moxa IKS and EDS, which may allow for the execution of unauthorized actions on the device. CVE ID: CVE-2019-6561	N/A	O-MOX-EDS 040419/701
N/A	05-03-2019	10	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password, which could lead to a full compromise of the device. CVE ID: CVE-2019-6563	N/A	O-MOX-EDS 040419/702
N/A	05-03-2019	4.3	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be used to send a malicious script. CVE ID: CVE-2019-6565	N/A	O-MOX-EDS 040419/703
eds-408a_firr	nware				
N/A	05-03-2019	5	Moxa IKS and EDS store plaintext passwords, which may allow sensitive information to be read by someone with access to the device.	N/A	O-MOX-EDS 040419/704

 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-2019-6518		
N/A	05-03-2019	5	Moxa IKS and EDS does not properly check authority on server side, which results in a readonly user being able to perform arbitrary configuration changes. CVE ID: CVE-2019-6520	N/A	O-MOX-EDS 040419/705
N/A	05-03-2019	8.5	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot. CVE ID: CVE-2019-6522	N/A	O-MOX-EDS 040419/706
N/A	05-03-2019	5	Moxa IKS and EDS do not implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack. CVE ID: CVE-2019-6524	N/A	O-MOX-EDS 040419/707
N/A	05-03-2019	7.5	Several buffer overflow vulnerabilities have been identified in Moxa IKS and EDS, which may allow remote code execution. CVE ID: CVE-2019-6557	N/A	O-MOX-EDS 040419/708

Vulnerability Type(s)	Publish Date	cvss		Descript	ion & CV	E ID	Pa	atch	NCI	IPC ID
N/A	05-03-2019	4	rem user serv craf caus	ote aut rs to cau vice via ted pac se the sv	nd EDS a henticat use a der a specia ket, whi witch to E-2019	ed nial of lly ch may crash.	N/A			X-EDS 19/709
N/A	05-03-2019	6.8	Cross-site request forgery has been identified in Moxa IKS and EDS, which may allow for the execution of unauthorized actions on the device. CVE ID: CVE-2019-6561				N/A			X-EDS 19/710
N/A	05-03-2019	10	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password, which could lead to a full compromise of the device. CVE ID: CVE-2019-6563				N/A		O-MOX-EDS- 040419/711	
N/A	05-03-2019	4.3	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be used to send a malicious script. CVE ID: CVE-2019-6565			N/A			X-EDS 19/712	
eds-510a_firi	mware									
N/A	05-03-2019	5	_		nd EDS s issword		N/A		О-МО	X-EDS
CV Scoring Scal (CVSS)	0-1		2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Vulnerability Ty	pe(s): CSRF- Cross S Denial of Service;	-	_	-		_				on; DoS-

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			which may allow sensitive information to be read by someone with access to the device.		040419/713
			CVE ID : CVE-2019-6518		
N/A	05-03-2019	5	Moxa IKS and EDS does not properly check authority on server side, which results in a readonly user being able to perform arbitrary configuration changes.	N/A	O-MOX-EDS 040419/714
			CVE ID : CVE-2019-6520		
N/A	05-03-2019	8.5	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot.	N/A	O-MOX-EDS 040419/715
			CVE ID : CVE-2019-6522		
N/A	05-03-2019	5	Moxa IKS and EDS do not implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute force attack. CVE ID: CVE-2019-6524	N/A	O-MOX-EDS 040419/716
N/A	05-03-2019	7.5	Several buffer overflow vulnerabilities have been identified in Moxa IKS and	N/A	O-MOX-EDS 040419/717

Vulnerability Type(s)	Publish Date	CVSS	Descript	tion & CVI	E ID	Pa	tch	NCII	PC ID
			EDS, which	-					
			remote cod						
			CVE ID : CV	E-2019	-6557				
N/A	remote authenticusers to cause a construction of the construction				ial of ly ch may crash.	N/A			X-EDS 9/718
N/A	05-03-2019	6.8	Cross-site r has been id Moxa IKS an may allow f execution o actions on t	entified ind EDS, we consider the funauth the device the consideration of the consideration of the device the	in which orized e.	N/A			X-EDS 9/719
					.0301				
N/A	05-03-2019	10	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password, which could lead to a full compromise of the device. CVE ID: CVE-2019-6563			N/A			X-EDS 9/720
N/A	05-03-2019	4.3	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be used to send a malicious script. CVE ID: CVE-2019-6565		y validate user iving enticated and cicated attackers ity to perform XSS which may be send a malicious				X-EDS 9/721
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	Pat	tch	NCII	PC ID
iks-g6824a_fi	rmware						
N/A	05-03-2019	5	Moxa IKS and EDS store plaintext passwords, which may allow sensitive information to be read be someone with access to the device. CVE ID: CVE-2019-651	N/A		O-MOX 04041	_
			Moxa IKS and EDS does not properly check				
N/A	05-03-2019	5	authority on server side, which results in a read-only user being able to perform arbitrary configuration changes. CVE ID: CVE-2019-652	N/A		O-MOX 04041	
N/A	05-03-2019	8.5	Moxa IKS and EDS fails to properly check array bounds which may allow an attacker to read device memory on arbitrary addresses, and may allow an attacker to retrieve sensitive data or cause device reboot.	v ce		O-MOX-IKS 040419/724	
			CVE ID : CVE-2019-652	2			
N/A	05-03-2019	5	Moxa IKS and EDS do no implement sufficient measures to prevent multiple failed authentication attempts, which may allow an attacker to discover passwords via brute for attack. CVE ID: CVE-2019-652	N/A		O-MOX 04041	
CV Scoring Scal	e 0-1 1-	2 2	-3 3-4 4-5 5- 6	6 6-7	7-8	8-9	9-10
(CVSS) Vulnerability Ty			st Forgery; Dir. Trav Directory				

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
N/A	7/A 05-03-2019 7		Several buffer overflow vulnerabilities have been identified in Moxa IKS and EDS, which may allow remote code execution. CVE ID: CVE-2019-6557	N/A	O-MOX-IKS 040419/726
N/A	Moxa IKS and EDS allow remote authenticated users to cause a denial of service via a specially crafted packet, which makes the switch to crash		users to cause a denial of	N/A	O-MOX-IKS 040419/727
N/A	Cross-site request forge has been identified in Moxa IKS and EDS, which may allow for the execution of unauthoriz actions on the device.		Moxa IKS and EDS, which may allow for the execution of unauthorized	N/A	O-MOX-IKS 040419/728
N/A	Moxa IKS and EDS generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password which could lead to a full compromise of the device		generate a predictable cookie calculated with an MD5 hash, allowing an attacker to capture the administrator's password,	N/A	O-MOX-IKS 040419/729
N/A	05-03-2019	4.3	Moxa IKS and EDS fails to properly validate user input, giving unauthenticated and authenticated attackers the ability to perform XSS attacks, which may be	N/A	O-MOX-IKS 040419/730

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			used to send a malicious script.		
			CVE ID : CVE-2019-6565		
Nokia					
i-240w-q_gpo	on_ont_firmwar	e		1	
N/A	05-03-2019	5	The Alcatel Lucent I- 240W-Q GPON ONT using firmware version 3FE54567BOZJ19 allows a remote, unauthenticated attacker to enable telnetd on the router via a crafted HTTP request. CVE ID: CVE-2019-3917	N/A	O-NOK-I-24- 040419/731
N/A	05-03-2019	10	The Alcatel Lucent I- 240W-Q GPON ONT using firmware version 3FE54567BOZJ19 contains multiple hard coded credentials for the Telnet and SSH interfaces.	N/A	O-NOK-I-24- 040419/732
			CVE ID : CVE-2019-3918		
N/A	05-03-2019	6.5	The Alcatel Lucent I- 240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/usb_restore_F orm?script/. CVE ID: CVE-2019-3919	N/A	O-NOK-I-24- 040419/733
N/A	05-03-2019	6.5	The Alcatel Lucent I- 240W-Q GPON ONT using	N/A	0-NOK-I-24- 040419/734

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID
			firmware version 3FE54567BOZJ19 is vulnerable to authenticated command injection via crafted HTTP request sent by a remote, authenticated attacker to /GponForm/device_Form? script/. CVE ID: CVE-2019-3920		
N/A	05-03-2019	6.5	The Alcatel Lucent I- 240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, authenticated attacker to /GponForm/usb_Form?scr ipt/. An attacker can leverage this vulnerability to potentially execute arbitrary code. CVE ID: CVE-2019-3921	N/A	O-NOK-I-24- 040419/735
N/A	05-03-2019	7.5	The Alcatel Lucent I- 240W-Q GPON ONT using firmware version 3FE54567BOZJ19 is vulnerable to a stack buffer overflow via crafted HTTP POST request sent by a remote, unauthenticated attacker to /GponForm/fsetup_Form. An attacker can leverage	N/A	O-NOK-I-24- 040419/736

Publish Date	CVSS	Description & CVE ID				Pa	atch	NCII	IPC ID
		pote arbi	entially trary co	execute ode.					
ct		UV E	. 12 . 0.	2 2017	3722				
ty_proxy_firm	ware								
05-03-2019	6.5	Telese Smart From Gates 4.2 6.0 Telese MU 5.1 and TCG 5.1 and Vers The brow as a or V allow exection.	econtrolart Telectily, IEC1 exy versiceway 30 21, 5.0.2 16 and pecontrol Version 19, 6.0.1 Telecon Version 19, 6.0.1 EC104 sion 2.2 web ap wser interior ctive HT CBScript w an attented	Gatewal control (104 Security of Security 10 and plication) and plication of the control of the	y and Jnit rity control as P, d y XS- , 5.0.27, rior, eway 5.0.27, rior, rol Unit r, rior, y Proxy prior a script, could	N/A		O-PSI- 04041	-IEC1- 19/737
05-03-2019	5					N/A		O-SAG F@ST	
9 04 4	-2 2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	ty_proxy_firmv 05-03-2019 mware 05-03-2019	05-03-2019 6.5 mware 05-03-2019 5	this pote arbi CVE ty_proxy_firmware PSI Tele Sma fam Property (a.c.) (a.c.) (b.c.) (b.c.) (c.c.) (c.c.	this vulnera potentially arbitrary concept to the potential potential process. The potential process of the potential proce	this vulnerability to potentially execute arbitrary code. CVE ID : CVE-2019 Et ty_proxy_firmware PSI GridConnect Gm Telecontrol Gatewas Smart Telecontrol Uffamily, IEC104 Secuproxy versions Tele Gateway 3G Version 4.2.21, 5.0.27, 5.1.19 6.0.16 and prior, an Telecontrol Gatewas MU Versions 4.2.21, 5.1.19, 6.0.16 and prior and Telecontrol Gatewas VM Versions 4.2.21, 5.1.19, 6.0.16 and prior and Smart Telecontrol Gatewas VM Versions 5.0.27 5.1.19, 6.0.16 and prior and IEC104 Security Version 2.2.10 and prior a	this vulnerability to potentially execute arbitrary code. CVE ID : CVE-2019-3922 Typroxy_firmware PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and IEC104 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code. CVE ID : CVE-2019-6528 mware 05-03-2019 5 Sagemcom F@st 5260 routers using firmware	this vulnerability to potentially execute arbitrary code. CVE ID : CVE-2019-3922 Typroxy_firmware PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and IEC104 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code. CVE ID : CVE-2019-6528 mware 05-03-2019 5 Sagemcom F@st 5260 routers using firmware	this vulnerability to potentially execute arbitrary code. CVE ID: CVE-2019-3922 Typroxy_firmware PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and IEC104 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code. CVE ID: CVE-2019-6528 mware 05-03-2019 5 Sagemcom F@st 5260 routers using firmware	this vulnerability to potentially execute arbitrary code. CVE ID: CVE-2019-3922 PSI GridConnect GmbH Telecontrol Gateway and Smart Telecontrol Unit family, IEC104 Security Proxy versions Telecontrol Gateway 3G Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway XS-MU Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Telecontrol Gateway VM Versions 4.2.21, 5.0.27, 5.1.19, 6.0.16 and prior, and Smart Telecontrol Unit TCG Versions 5.0.27, 5.1.19, 6.0.16 and prior, and Bictlo4 Security Proxy Version 2.2.10 and prior The web application browser interprets input as active HTML, JavaScript, or VBScript, which could allow an attacker to execute arbitrary code. CVE ID: CVE-2019-6528 mware 05-03-2019 Sagemcom F@st 5260 N/A O-SAC F@ST

Vulnerability Type(s)	Publish Date	cvss	Description & CVE ID	Patch	NCIIPC ID						
			version 0.4.39, in WPA mode, default to using a PSK that is generated from a 2-part wordlist of known values and a nonce with insufficient entropy. The number of possible PSKs is about 1.78 billion, which is too small. CVE ID: CVE-2019-9555		040419/738						
tengcon t-920_plc_firmware											
N/A	06-03-2019	5	An issue was discovered on TENGCONTROL T-920 PLC v5.5 devices. It allows remote attackers to cause a denial of service (persistent failure mode) by sending a series of \x19\xb2\x00\x00\x00\x00\x00\x00\x00\x00\x00\x0	N/A	O-TEN-T-92- 040419/739						
Zyxel											
nbg-418n_firmware											
N/A	07-03-2019	6.8	Zyxel NBG-418N v2 v1.00(AAXM.4)C0 devices allow login.cgi CSRF. CVE ID: CVE-2019-6710	N/A	0-ZYX-NBG 040419/740						

CV Scoring Scale	0-1	1.2	2 2	2.4	<i>1</i> E	5.6	6.7	7.0	0.0	0.10
(CVSS)	0-1	1-2	2-3	5-4	4-5	5-0	6-7	7-0	0-9	9-10