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	Description & CVE ID	Patch	NCIIPC ID
Application					
1024tools					
1024tools					
N/A	12-03-2019	4.3	DOM-based XSS exists in 1024Tools Markdown 1.0 via vectors involving the '<EMBED SRC="data:image/svg+xml' substring. **CVE ID : CVE-2019-9736**	N/A	A-102-1024-040419/1
1234n					
minicms					
N/A	06-03-2019	5.8	MiniCMS 1.10 allows mc-admin/post.php?state=publish&delete= CSRF to delete articles, a different vulnerability than CVE-2018-18891. **CVE ID : CVE-2019-9603**	N/A	A-123-MINI-040419/2
Airdroid					
Airdroid					
N/A	06-03-2019	7.8	The AirDroid application through 4.2.1.6 for Android allows remote attackers to cause a denial of service (service crash) via many simultaneous sdctl/comm/lite_auth/ requests. **CVE ID : CVE-2019-9599**	N/A	A-AIR-AIRD-040419/3

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
airdrop_project					
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
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=PhoneRequestAuthorization requests. **CVE ID : CVE-2019-9831**	N/A	A-AIR-AIRM-040419/5
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	Description & CVE ID	Patch	NCIIPC ID
			Distributed mode. Note that versions before 4.0 are not able to encrypt traffic between the nodes, nor authenticate the participating nodes so upgrade to JMeter 5.1 is also advised. **CVE ID : CVE-2019-0187**		
qpid_broker-j					
N/A	06-03-2019	5	A Denial of Service vulnerability was found in Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 which allows an unauthenticated attacker to crash the broker instance by sending specially crafted commands using AMQP protocol versions below 1.0 (AMQP 0-8, 0-9, 0-91 and 0-10). Users of Apache Qpid Broker-J versions 6.0.0-7.0.6 (inclusive) and 7.1.0 utilizing AMQP protocols 0-8, 0-9, 0-91, 0-10 must upgrade to Qpid Broker-J versions 7.0.7 or 7.1.1 or later. **CVE ID : CVE-2019-0200**	N/A	A-APA-QPID-040419/7
Solr					
N/A	07-03-2019	7.5	In Apache Solr versions 5.0.0 to 5.5.5 and 6.0.0 to 6.6.5, the Config API allows to configure the JMX server via an HTTP POST	N/A	A-APA-SOLR-040419/8

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request. By pointing it to a malicious RMI server, an attacker could take advantage of Solr's unsafe deserialization to trigger remote code execution on the Solr side. **CVE ID : CVE-2019-0192**		
apowersoft					
apowermanager					
N/A	06-03-2019	5	The ApowerManager application through 3.1.7 for Android allows remote attackers to cause a denial of service via many simultaneous /?Key=PhoneRequestAuthorization requests. **CVE ID : CVE-2019-9601**	N/A	A-APO-APOW-040419/9
appcms					
appcms					
N/A	06-03-2019	4.3	AppCMS 2.0.101 allows XSS via the upload/callback.php params parameter. **CVE ID : CVE-2019-9595**	N/A	A-APP-APPC-040419/10
Apple					
Safari					
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	N/A	A-APP-SAFA-040419/11

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. **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. **CVE ID : CVE-2019-6215**	N/A	A-APP-SAFA-040419/12
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**	https://support.apple.com/HT209451	A-APP-SAFA-040419/13
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,	https://support.apple.com/HT209451	A-APP-SAFA-040419/14

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-6217**		
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-2019-6226**	https://support.apple.com/HT209451	A-APP-SAFA-040419/15
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**	https://support.apple.com/HT209451	A-APP-SAFA-040419/16
N/A	05-03-2019	4.3	A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation.	https://support.apple.com/HT20944	A-APP-SAFA-040419/17

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	9	
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://support.apple.com/HT209451	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. Processing maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-6233**	https://support.apple.com/HT209451	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://support.apple.com/HT20945	A-APP-SAFA-040419/20

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	
Icloud					
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.com/HT209451	040419/23
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-2019-6217**	https://support.apple.com/HT209451	A-APP-ICLO-040419/24
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://support.apple.com/HT209451	A-APP-ICLO-040419/25

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-6226		
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://support.apple.com/HT209451	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://support.apple.com/HT209451	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://support.apple.com/HT209451	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://support.apple.com/HT209451	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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. **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. **CVE ID : CVE-2019-6216**	https://support.apple.com/HT209451	A-APP-ITUN-040419/32
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-2019-6217**	https://support.apple.com/HT209451	A-APP-ITUN-040419/33
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,	https://support.apple.com/HT209450	A-APP-ITUN-040419/34

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			iTunes 12.9.3 for Windows. A malicious application may be able to elevate privileges. **CVE ID : CVE-2019-6221**		
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-2019-6226**	https://support.apple.com/HT209451	A-APP-ITUN-040419/35
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://support.apple.com/HT209451	A-APP-ITUN-040419/36
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	https://support.apple.com/HT209451	A-APP-ITUN-040419/37

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	05-03-2019	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://support.apple.com/HT209451	A-APP-ITUN-040419/38
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://support.apple.com/HT209451	A-APP-ITUN-040419/39
axiosys					
bento4					
N/A	01-03-2019	6.8	An issue was discovered in	N/A	A-AXI-BENT-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bento4 1.5.1-628. An out of bounds write occurs in AP4_CttsTableEntry::AP4_CttsTableEntry() located in Core/Ap4Array.h. It can be triggered by sending a crafted file to (for example) the mp42hls binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9544**		040419/40
blog_mini_project					
blog_mini					
N/A	14-03-2019	4.3	In Blog_mini 1.0, XSS exists via the author name of a comment reply in the app/main/views.py articleDetails() function, related to app/templates/_article_comments.html. **CVE ID : CVE-2019-9765**	N/A	A-BLO-BLOG-040419/41
bluecms_project					
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 Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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 uploads. **CVE ID : CVE-2019-9563**	N/A	A-BLU-BLUE-040419/43
Bolt					
Bolt					
N/A	07-03-2019	6.5	Controller/Async/FilesystemManager.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 Scale (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cisco					
application_policy_infrastructure_controller					
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**	N/A	A-CIS-APPL-040419/47
enterprise_chat_and_email					
N/A	11-03-2019	4.3	Multiple vulnerabilities in	N/A	A-CIS-ENTE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the web-based management interface of Cisco Enterprise Chat and Email could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of the affected software. The vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit these vulnerabilities either by injecting malicious code in a chat window or by sending a crafted link to a user of the interface. In both cases, the attacker must persuade the user to click the crafted link or open the chat window that contains the attacker's code. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Version 11.6(1) is affected. **CVE ID : CVE-2019-1702**		040419/48
Cleanersoft					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
free_mp3_cd_ripper					
N/A	14-03-2019	6.8	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted .mp3 file. **CVE ID : CVE-2019-9766**	N/A	A-CLE-FREE-040419/49
N/A	14-03-2019	6.8	Stack-based buffer overflow in Free MP3 CD Ripper 2.6, when converting a file, allows user-assisted remote attackers to execute arbitrary code via a crafted .wma file. **CVE ID : CVE-2019-9767**	N/A	A-CLE-FREE-040419/50
Cmsmadesimple					
cms_made_simple					
N/A	11-03-2019	5	class.showtime2_image.php 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**	N/A	A-CMS-CMS_-040419/51
N/A	11-03-2019	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-CMS_-040419/52

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			_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_server					
N/A	12-03-2019	4.3	Ability Mail Server 4.2.6 has Persistent Cross Site Scripting (XSS) via the body e-mail body. 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-2019-9557**	N/A	A-COD-ABIL-040419/53
cyberark					
endpoint_privilege_manager					
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-040419/54

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges) to escalate privileges or crash the machine by loading an image, such as a DLL, with a long path. **CVE ID : CVE-2019-9627**		
dhcms_project					
dhcms					
N/A	03-03-2019	3.5	DhCms through 2017-09-18 has admin.php?r=admin/Index/index XSS. **CVE ID : CVE-2019-9550**	N/A	A-DHC-DHCM-040419/55
dilicms					
dilicms					
N/A	07-03-2019	3.5	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 site_name. **CVE ID : CVE-2019-8438**	N/A	A-DIL-DILI-040419/56
N/A	07-03-2019	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. **CVE ID : CVE-2019-8439**	N/A	A-DIL-DILI-040419/57
N/A	07-03-2019	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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the third textbox (aka site logo) of "System setting->site setting" of admin/index.php, aka site_logo. **CVE ID : CVE-2019-8440**		
Directadmin					
Directadmin					
N/A	07-03-2019	6.8	JBMC DirectAdmin 1.55 allows CSRF via the /CMD_ACCOUNT_ADMIN URI to create a new admin account. **CVE ID : CVE-2019-9625**	N/A	A-DIR-DIRE-040419/59
dradisframework					
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-040419/60
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-EBRI-040419/61

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter, as demonstrated by reading the user-data/save/backup.sql file. **CVE ID : CVE-2019-9622**		
editor.md_project					
editor.md					
N/A	12-03-2019	4.3	Editor.md 1.5.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml ' substring. **CVE ID : CVE-2019-9737**	N/A	A-EDI-EDIT-040419/62
esafenet					
electronic_document_security_management_system					
N/A	08-03-2019	5	ESAFENET CDG V3 and V5 has an arbitrary file download vulnerability via the fileName parameter in download.jsp because the InstallationPack parameter is mishandled in a /CDGServer3/ClientAjax request. **CVE ID : CVE-2019-9632**	N/A	A-ESA-ELEC-040419/63
F5					
big-ip_access_policy_manager					
N/A	13-03-2019	5	In BIG-IP 14.0.0-14.0.0.2, 13.0.0-13.1.1.1, 12.1.0-12.1.3.6, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, when processing fragmented ClientHello messages in a DTLS session TMM may	https://support.f5.com/csp/article/K97241515	A-F5-BIG--040419/64

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://support.f5.com/csp/article/K29280193	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://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/66

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cannot login and does not have the access level to perform the attack. **CVE ID : CVE-2019-6598**		
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 cross-site scripting (XSS) attack. **CVE ID : CVE-2019-6599**	https://support.f5.com/csp/article/K46401178	A-F5-BIG--040419/67
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/68
big-ip_advanced_firewall_manager					
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-	https://support.f5.com/cs	A-F5-BIG--040419/69

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/K29280193	
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://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	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_analytics					
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://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/72
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://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/73

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/74
big-ip_application_acceleration_manager					
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	https://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/75

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**		
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://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/77

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**		
N/A	13-03-2019	2.1	In BIG-IP 13.0.0, 12.1.0-12.1.3.7, 11.6.1-11.6.3.2, or 11.5.1-11.5.8, the Application Acceleration Manager (AAM) wamd process used in processing of images and PDFs fails to drop group permissions when executing helper scripts. **CVE ID : CVE-2019-6601**	https://support.f5.com/csp/article/K25359902	A-F5-BIG--040419/78
big-ip_application_security_manager					
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://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/79
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	https://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/80

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/81
big-ip_domain_name_system					
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	https://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/82

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. **CVE ID : CVE-2019-6598**	https://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/84

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_edge_gateway					
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://support.f5.com/csp/article/K29280193	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://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/86

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/87
big-ip_fraud_protection_service					
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,	https://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/88

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-6598**	https://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	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_manager					
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://support.f5.com/csp/article/K29280193	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://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/92

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			perform the attack. **CVE ID : CVE-2019-6598**		
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/93
big-ip_link_controller					
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://support.f5.com/csp/article/K29280193	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://support.f5.com/cs	A-F5-BIG--040419/95

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	p/article/K44603900	
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/96
big-ip_local_traffic_manager					
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-	https://support.f5.com/cs	A-F5-BIG--040419/97

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/K29280193	
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://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	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**		
big-ip_policy_enforcement_manager					
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://support.f5.com/csp/article/K29280193	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://support.f5.com/csp/article/K44603900	A-F5-BIG--040419/101

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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 against unauthenticated clients. **CVE ID : CVE-2019-6600**	https://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/102
big-ip_webaccelerator					
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	https://support.f5.com/csp/article/K29280193	A-F5-BIG--040419/103

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**		
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://support.f5.com/csp/article/K44603900	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://support.f5.com/csp/article/K23734425	A-F5-BIG--040419/105

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			page. This can lead to a cross-site scripting attack against unauthenticated clients. **CVE ID : CVE-2019-6600**		
enterprise_manager					
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://support.f5.com/csp/article/K29280193	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 role). The No Access user role	https://support.f5.com/csp/article/K44603900	A-F5-ENTE-040419/107

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cannot login and does not have the access level to perform the attack. **CVE ID : CVE-2019-6598**		
feifeicms					
feifeicms					
N/A	14-03-2019	7.5	FeiFeiCMS 4.1.190209 allows remote attackers to upload and execute arbitrary PHP code by visiting index.php?s=Admin-Index to modify the set of allowable file extensions, as demonstrated by adding php to the default jpg,gif,png,jpeg setting, and then using the "add article" feature. **CVE ID : CVE-2019-9825**	N/A	A-FEI-FEIF-040419/108
Fengoffice					
feng_office					
N/A	07-03-2019	7.5	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. **CVE ID : CVE-2019-9623**	N/A	A-FEN-FENG-040419/109
Ffmpeg					
Ffmpeg					
N/A	12-03-2019	4.3	In FFmpeg 4.1, a denial of service in the subtitle decoder allows attackers to hog the CPU via a	N/A	A-FFM-FFMP-040419/110

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::readGenericBitmap() 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	Description & CVE ID	Patch	NCIIPC ID
			binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. This is related to JArithmeticDecoder::decodeBit. **CVE ID : CVE-2019-9543**		
N/A	01-03-2019	6.8	An issue was discovered in Poppler 0.74.0. A recursive function call, in JBIG2Stream::readTextRegion() located in JBIG2Stream.cc, 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. This is related to JBIG2Bitmap::clearToZero. **CVE ID : CVE-2019-9545**	N/A	A-FRE-POPP-040419/114
N/A	08-03-2019	7.5	Poppler 0.74.0 has a heap-based buffer over-read in the CairoRescaleBox.cc downsample_row_box_filter function. **CVE ID : CVE-2019-9631**	N/A	A-FRE-POPP-040419/115
Ftpgetter					
Ftpgetter					
N/A	13-03-2019	7.5	FTPGetter Standard v.5.97.0.177 allows remote	N/A	A-FTP-FTPG-040419/116

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code execution when a user initiates an FTP connection to an attacker-controlled machine that sends crafted responses. Long responses can also crash the FTP client with memory corruption. **CVE ID : CVE-2019-9760**		
gitnoteapp					
gitnote					
N/A	14-03-2019	6.8	gitnote 3.1.0 allows remote attackers to execute arbitrary code via a crafted Markdown file, as demonstrated by a javascript:window.parent.top.require('child_process').execFile substring in the onerror attribute of an IMG element. **CVE ID : CVE-2019-9785**	N/A	A-GIT-GITN-040419/117
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-XPDF-040419/118

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This is related to Catalog::countPageTree. **CVE ID : CVE-2019-9587**		
N/A	06-03-2019	6.8	There is an Invalid memory access in gAtomicIncrement() located at GMutex.h in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9588**	N/A	A-GLY-XPDF-040419/119
N/A	06-03-2019	6.8	There is a NULL pointer dereference vulnerability in PSOutputDev::setupResources() located in PSOutputDev.cc in Xpdf 4.01. It can be triggered by sending a crafted pdf file to (for example) the pdftops binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact. **CVE ID : CVE-2019-9589**	N/A	A-GLY-XPDF-040419/120
Gnome					
Glib					
N/A	08-03-2019	4.3	gio/gsocketclient.c in GNOME GLib 2.59.2 does	N/A	A-GNO-GLIB-040419/121

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 allows remote attackers to cause a denial of service (g_socket_client_connected_callback mishandling and application crash) via a crafted web site, as demonstrated by GNOME Web (aka Epiphany). **CVE ID : CVE-2019-9633**		
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 at bits.c. **CVE ID : CVE-2019-9771**	N/A	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

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 heap-based 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	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 (later than CVE-2019-9779). **CVE ID : CVE-2019-9776**	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 heap-based 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 heap-based 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					
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)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			url parameter, as demonstrated by the second argument to http.NewRequest with \r\n followed by an HTTP header or a Redis command. **CVE ID : CVE-2019-9741**		
golangtc					
gopher					
N/A	12-03-2019	4.3	jimmykuu Gopher 2.0 has DOM-based XSS via vectors involving the '<EMBED SRC="data:image/svg+xml' substring. **CVE ID : CVE-2019-9738**	N/A	A-GOL-GOPH-040419/134
IBM					
sterling_b2b_integrator					
N/A	05-03-2019	3.5	IBM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 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-ForceID: 155905. **CVE ID : CVE-2019-4027**	https://www.ibm.com/support/docview.wss?uid=ibm10874246	A-IBM-STER-040419/135
N/A	05-03-2019	3.5	IBM Sterling B2B Integrator 5.2.0.1 through	https://www.ibm.com/s	A-IBM-STER-040419/136

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.0.0.0 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: 155906. **CVE ID : CVE-2019-4028**	upport/docview.wss?uid=ibm10874246	
N/A	05-03-2019	3.5	IBM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 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: 155907. **CVE ID : CVE-2019-4029**	https://www.ibm.com/support/docview.wss?uid=ibm10874246	A-IBM-STER-040419/137
N/A	05-03-2019	4.3	IBM Sterling B2B Integrator 5.2.0.1 through 6.0.0.0 Standard Edition could allow highly sensitive information to be transmitted in plain text. An attacker could obtain this information using man in the middle techniques. IBM X-ForceID: 157008. **CVE ID : CVE-2019-4063**	https://www.ibm.com/support/docview.wss?uid=ibm10874234	A-IBM-STER-040419/138

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
websphere_application_server					
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-040419/139
websphere_virtual_enterprise					
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-040419/140
financial_transaction_manager					
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)	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
			injection. A remote attacker could send specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-ForceID: 155998. **CVE ID : CVE-2019-4032**		
content_navigator					
N/A	14-03-2019	6.5	IBM Content Navigator 3.0CD is could allow an attacker to execute arbitrary code on a user's workstation. When editing an executable file in ICN with Edit service, it will be executed on the user's workstation. IBM X-Force ID: 156000. **CVE ID : CVE-2019-4034**	https://www.ibm.com/support/docview.wss?uid=ibm10869066	A-IBM-CONT-040419/142
DB2					
N/A	11-03-2019	7.2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 155893. **CVE ID : CVE-2019-4015**	https://www.ibm.com/support/docview.wss?uid=ibm10740413	A-IBM-DB2-040419/143
N/A	11-03-2019	7.2	IBM DB2 for Linux, UNIX	https://ww	A-IBM-DB2-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 155894. **CVE ID : CVE-2019-4016**	w.ibm.com/support/docview.wss?uid=ibm10740413	040419/144
ichain					
insurance_wallet					
N/A	12-03-2019	5	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**	N/A	A-ICH-INSU-040419/145
Imagemagick					
Imagemagick					
N/A	07-03-2019	5	In ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c. **CVE ID : CVE-2019-7175**	N/A	A-IMA-IMAG-040419/146
Intel					
matrix_storage_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://www.intel.com/content/www/us/en/sec	A-INT-MATR-040419/147

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0121**	urity-center/advisory/INTEL-SA-00216.html	
usb_3.0_creator_utility					
N/A	14-03-2019	4.6	Improper permissions for Intel(R) USB 3.0 Creator Utility all versions may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2019-0129**	https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00229.html	A-INT-USB_-040419/148
rapid_storage_technology_enterprise					
N/A	14-03-2019	4.6	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. **CVE ID : CVE-2019-0135**	https://www.intel.com/content/www/us/en/security-center/advisory/INTEL-SA-00231.html	A-INT-RAPI-040419/149
iotivity					
iotivity					
N/A	13-03-2019	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-IOTI-040419/150

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bigger than spoofed requests. This occurs because the construction of a "4.01 Unauthorized" response is mishandled. NOTE: the vendor states "While this is an interesting attack, there is no plan for maintainer to fix, as we are migrating to IoTivity Lite." **CVE ID : CVE-2019-9750**		
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/jenkinsci/plugins/scriptsecurity/sandbox/groovy/GroovySandbox.java, src/main/java/org/jenkinsci/plugins/scriptsecurity/sandbox/groovy/SecureGroovyScript.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM. **CVE ID : CVE-2019-1003029**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1336%20(1)	A-JEN-SCRI-040419/151
pipeline_groovy					
N/A	08-03-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Pipeline: Groovy	https://jenkins.io/security/advisory/2	A-JEN-PIPE-040419/152

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Plugin 2.63 and earlier in pom.xml, src/main/java/org/jenkinsci/plugins/workflow/cps/CpsGroovyShell.java that allows attackers able to control pipeline scripts to execute arbitrary code on the Jenkins master JVM. **CVE ID : CVE-2019-1003030**	019-03-06/#SECURITY-1336%20(2)	
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/plugins/groovy/StringScriptSource.java that allows attackers with Overall/Read permission to execute arbitrary code on the Jenkins master JVM. **CVE ID : CVE-2019-1003033**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1338	A-JEN-GROO-040419/153
matrix_project					
N/A	08-03-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Matrix Project Plugin 1.13 and earlier in pom.xml, src/main/java/hudson/matrix/FilterScript.java that allows attackers with Job/Configure permission to execute arbitrary code	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1339	A-JEN-MATR-040419/154

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the Jenkins master JVM. **CVE ID : CVE-2019-1003031**		
email_extension					
N/A	08-03-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Email Extension Plugin 2.64 and earlier in pom.xml, src/main/java/hudson/plugins/emailext/ExtendedEmailPublisher.java, src/main/java/hudson/plugins/emailext/plugins/content/EmailExtScript.java, src/main/java/hudson/plugins/emailext/plugins/content/ScriptContent.java, src/main/java/hudson/plugins/emailext/plugins/trigger/AbstractScriptTrigger.java that allows attackers with Job/Configure permission to execute arbitrary code on the Jenkins master JVM. **CVE ID : CVE-2019-1003032**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1340	A-JEN-EMAI-040419/155
job_dsl					
N/A	08-03-2019	6.5	A sandbox bypass vulnerability exists in Jenkins Job DSL Plugin 1.71 and earlier in job-dsl-core/src/main/groovy/javaposse/jobdsl/dsl/AbstractDslScriptLoader.groovy, job-dsl-	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1342	A-JEN-JOB_-040419/156

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			plugin/build.gradle, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/JobDslWhitelist.groovy, job-dsl-plugin/src/main/groovy/javaposse/jobdsl/plugin/SandboxDslScriptLoader.groovy that allows attackers with control over Job DSL definitions to execute arbitrary code on the Jenkins master JVM. **CVE ID : CVE-2019-1003034**		
azure_vm_agents					
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/microsoft/azure/vmagent/AzureVMAgentTemplate.java, src/main/java/com/microsoft/azure/vmagent/AzureVMCloud.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://jenkins.io/security/advisory/2019-03-06/#SECURITY-1330	A-JEN-AZUR-040419/157

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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/microsoft/azure/vmagent/AzureVMAgent.java that allows attackers with Overall/Read permission to attach a public IP address to an Azure VM agent. **CVE ID : CVE-2019-1003036**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1331	A-JEN-AZUR-040419/158
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/microsoft/azure/vmagent/AzureVMCloud.java that allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins. **CVE ID : CVE-2019-1003037**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1332	A-JEN-AZUR-040419/159
repository_connector					
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/repositoryconnector/ArtifactDeploy	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-958	A-JEN-REPO-040419/160

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			er.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/Repository.java, src/main/java/org/jvnet/hudson/plugins/repositoryconnector/UserPwd.java that allows an attacker with local file system access or control of a Jenkins administrator's web browser (e.g. malicious extension) to retrieve the password stored in the plugin configuration. **CVE ID : CVE-2019-1003038**		
appdynamics					
N/A	08-03-2019	4	An insufficiently protected credentials vulnerability exists in JenkinsAppDynamics Dashboard Plugin 1.0.14 and earlier in src/main/java/nl/codecentric/jenkins/appd/AppDynamicsResultsPublisher.java that allows attackers without permission to obtain passwords configured in jobs to obtain them. **CVE ID : CVE-2019-1003039**	https://jenkins.io/security/advisory/2019-03-06/#SECURITY-1087	A-JEN-APPD-040419/161
Joomla					

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-JOO-JOOM-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-JOO-JOOM-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. **CVE ID : CVE-2019-9713**	N/A	A-JOO-JOOM-040419/164
N/A	12-03-2019	4.3	An issue was discovered in Joomla! before 3.9.4. The media form field lacks escaping, leading to XSS. **CVE ID : CVE-2019-9714**	N/A	A-JOO-JOOM-040419/165
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.php?type=action&action=bat	N/A	A-JTB-JTBC-040419/166

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_manager					
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::startElement 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

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
maccms					
N/A	14-03-2019	6.5	Maccms 10 allows remote attackers to execute arbitrary PHP code by entering this code in a template/default_pc/html/art Edit action. This occurs because template rendering uses an include operation on a cache file, which bypasses the prohibition of .php files as templates. **CVE ID : CVE-2019-9829**	N/A	A-MAC-MACC-040419/170
Mailtraq					
webmail					
N/A	12-03-2019	4.3	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**	N/A	A-MAI-WEBM-040419/171
Mcafee					
database_security					
N/A	12-03-2019	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	https://kc.mcafee.com/corporate/index?page=content&id=SB10277	A-MCA-DATA-040419/172

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			incorrectly auto completing password fields in the admin browser login screen. **CVE ID : CVE-2019-3615**		
medical_store_script_project					
medical_store_script					
N/A	06-03-2019	5	PHP Scripts Mall Medical Store Script 3.0.3 allows Path Traversal by navigating to the parent directory of a jpg or png file. **CVE ID : CVE-2019-9607**	N/A	A-MED-MEDI-040419/173
Microsoft					
Excel					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669	A-MIC-EXCE-040419/174
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540	A-MIC-EXCE-040419/175

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0540**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669	A-MIC-EXCE-040419/176
office_365_proplus					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540	A-MIC-OFFI-040419/177
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669	A-MIC-OFFI-040419/178
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when	https://portal.msrc.micr	A-MIC-OFFI-

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/advisory/CVE-2019-0671	040419/179
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-2019-0675. **CVE ID : CVE-2019-0672**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0674	A-MIC-OFFI-040419/182
powerpoint_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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540	A-MIC-POWE-040419/183
word_viewer					
N/A	05-03-2019	4.3	A security feature bypass	https://port	A-MIC-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540	WORD-040419/184
chakracore					
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-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0590**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0590	A-MIC-CHAK-040419/185
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0591	A-MIC-CHAK-040419/186

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0644, 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-2019-0591, 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-2019-0655. **CVE ID : CVE-2019-0593**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0640, 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-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0607**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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. **CVE ID : CVE-2019-0610**		
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-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0640**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0642	A-MIC-CHAK-040419/192

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0644, 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-2019-0591, 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.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-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0651**	guidance/advisory/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-2019-0591, 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-2019-0655. **CVE ID : CVE-2019-0652**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/ad	A-MIC-CHAK-040419/197

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652. **CVE ID : CVE-2019-0655**	visory/CVE-2019-0655	
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0658	A-MIC-CHAK-040419/198
sharepoint_server					
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.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0594	A-MIC-SHAR-040419/199

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0594		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0604	A-MIC-SHAR-040419/200
sharepoint_enterprise_server					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0670	A-MIC-SHAR-040419/204
sharepoint_foundation					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0670	A-MIC-SHAR-040419/207
internet_explorer					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0676	A-MIC-INTE-040419/210
.net_framework					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0613	A-MIC-.NET-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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-.NET-040419/212

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. **CVE ID : CVE-2019-0657**	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'. **CVE ID : CVE-2019-0613**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0613	A-MIC-VISU-040419/213
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0657	A-MIC-VISU-040419/214
powershell_core					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0627	A-MIC-POWE-040419/215

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0632. **CVE ID : CVE-2019-0627**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0631	A-MIC-POWE-040419/216
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. **CVE ID : CVE-2019-0632**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0632	A-MIC-POWE-040419/217
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0657	A-MIC-POWE-040419/218
.net_core					
N/A	05-03-2019	4.3	A vulnerability exists in certain .Net Framework API's and Visual Studio in	https://portal.msrc.microsoft.com/en	A-MIC-.NET-040419/219

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/advisory/CVE-2019-0657	
office_compatibility_pack					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669	A-MIC-OFFI-040419/220
exchange_server					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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): 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	05-03-2019	9.3	A remote code execution vulnerability exists in Visual Studio Code when it process environment variables after opening a project, aka 'Visual Studio Code Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0728**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0728	A-MIC-VISU-040419/223
java_software_development_kit					
N/A	05-03-2019	7.5	An Elevation of Privilege vulnerability exists in the way Azure IoT Java SDK generates symmetric keys for encryption, allowing an attacker to predict the randomness of the key, aka 'Azure IoT Java SDK Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0729**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0729	A-MIC-JAVA-040419/224
N/A	05-03-2019	5	An information disclosure vulnerability exists in the way Azure IoT Java SDK logs sensitive information, aka 'Azure IoT Java SDK Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0741**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0741	A-MIC-JAVA-040419/225
team_foundation_server					
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-TEAM-040419/226

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0743. **CVE ID : CVE-2019-0742**	2019-0742	
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 ID is unique from CVE-2019-0742. **CVE ID : CVE-2019-0743**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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 attacker could send a victim a specially crafted file, which could trick the victim into entering credentials, aka	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540	A-MIC-OFFI-040419/229

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Microsoft Office Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0540**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669	A-MIC-OFFI-040419/230
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-2019-0672, CVE-2019-0673, CVE-2019-0674, CVE-2019-0675. **CVE ID : CVE-2019-0671**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0671	A-MIC-OFFI-040419/231
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0672	A-MIC-OFFI-040419/232

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0672, CVE-2019-0674, CVE-2019-0675. **CVE ID : CVE-2019-0673**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0673, CVE-2019-0675. **CVE ID : CVE-2019-0674**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0672, CVE-2019-0673, CVE-2019-0674. **CVE ID : CVE-2019-0675**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0675	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-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0590**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0590	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://portal.msrc.microsoft.com/en	A-MIC-EDGE-040419/237

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0591**	-US/security-guidance/advisory/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-2019-0591, 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-2019-0655. **CVE ID : CVE-2019-0593**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.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-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0605**	guidance/advisory/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-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0607**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/ad	A-MIC-EDGE-040419/241

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-0610**	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. **CVE ID : CVE-2019-0634**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0640	A-MIC-EDGE-040419/243

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652, CVE-2019-0655. **CVE ID : CVE-2019-0642**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0642	A-MIC-EDGE-040419/245
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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): 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-2019-0643		
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-2019-0591, 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.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-2019-0591, CVE-2019-0593, CVE-2019-0605, CVE-2019-0607, CVE-2019-0610, 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-2019-0591, 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-2019-0655. **CVE ID : CVE-2019-0652**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0607, CVE-2019-0610, CVE-2019-0640, CVE-2019-0642, CVE-2019-0644, CVE-2019-0651, CVE-2019-0652. **CVE ID : CVE-2019-0655**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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

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_onsite					
N/A	06-03-2019	4.3	A reflected Cross-site 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_project					
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 (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-5919**		040419/263
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_project					
njiandan-cms					
N/A	07-03-2019	6.8	njiandan-cms through 2013-05-23 has index.php/admin/user_new 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://www.openssl.org/news/secadv/2019030	A-OPE-OPEN-040419/266

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specifies that the nonce value (IV) should be 96 bits (12 bytes). OpenSSL allows a variable nonce length and front pads the nonce with 0 bytes if it is less than 12 bytes. However it also incorrectly allows a nonce to be set of up to 16 bytes. In this case only the last 12 bytes are significant and any additional leading bytes are ignored. It is a requirement of using this cipher that nonce values are unique. Messages encrypted using a reused nonce value are susceptible to serious confidentiality and integrity attacks. If an application changes the default nonce length to be longer than 12 bytes and then makes a change to the leading bytes of the nonce expecting the new value to be a new unique nonce then such an application could inadvertently encrypt messages with a reused nonce. Additionally the ignored bytes in a long nonce are not covered by the integrity guarantee of this cipher. Any application that relies on the integrity of these	6.txt	

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					
N/A	12-03-2019	4	An issue was discovered in the iptables firewall module in OpenStack Neutron before 10.0.8, 11.x before 11.0.7, 12.x before 12.0.6, and 13.x before 13.0.3. By setting a destination port in a	N/A	A-OPE-NEUT-040419/267

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			security group rule along with a protocol that doesn't support that option (for example, VRRP), an authenticated user may block further application of security group rules for instances from any project/tenant on the compute hosts to which it's applied. (Only deployments using the iptables security group driver are affected.) **CVE ID : CVE-2019-9735**		
openwsman_project					
openwsman					
N/A	14-03-2019	5	Openwsman, versions up to and including 2.6.9, are vulnerable to arbitrary file disclosure because the working directory of openwsmand daemon was set to root directory. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to openwsman server. **CVE ID : CVE-2019-3816**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3816	A-OPE-OPEN-040419/268
N/A	14-03-2019	5	Openwsman, versions up to and including 2.6.9, are vulnerable to infinite loop in process_connection() when parsing specially crafted HTTP requests. A	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3833	A-OPE-OPEN-040419/269

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote, unauthenticated attacker can exploit this vulnerability by sending malicious HTTP request to cause denial of service to openwsman server. **CVE ID : CVE-2019-3833**		
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**	N/A	A-OTR-OTRS-040419/270
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	N/A	A-OTR-OTRS-040419/271

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pload.pm. **CVE ID : CVE-2019-9752**		
personal_video_collection_script_project					
personal_video_collection_script					
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					
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_MAKERNOTE because of	N/A	A-PHP-PHP-040419/274

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_MAKERNOTE 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 Cross-site 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.php page has a reflected Cross-site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-7661**	N/A	A-PHP-PHPM-040419/280
phpshe					
phpshe					

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
N/A	13-03-2019	5	An XXE issue was 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/alipay/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://pivotal.io/security/cve-2019-3776	A-PIV-OPER-040419/284

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote user that is able to convince an Operations Manager user to interact with malicious content could execute arbitrary JavaScript in the user's browser. **CVE ID : CVE-2019-3776**		
spring_security_oauth					
N/A	07-03-2019	6.4	Spring Security OAuth, versions 2.3 prior to 2.3.5, and 2.2 prior to 2.2.4, and 2.1 prior to 2.1.4, and 2.0 prior to 2.0.17, and older unsupported versions could be susceptible to an open redirector attack that can leak an authorization code. A malicious user or attacker can craft a request to the authorization endpoint using the authorization code grant type, and specify a manipulated redirection URI via the "redirect_uri" parameter. This can cause the authorization server to redirect the resource owner user-agent to a URI under the control of the attacker with the leaked authorization code. This vulnerability exposes applications that meet all of the following requirements: Act in the	https://pivotal.io/security/cve-2019-3778	A-PIV-SPRI-040419/285

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			role of an Authorization Server (e.g. @EnableAuthorizationServer) 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					
N/A	08-03-2019	7.2	A local privilege escalation vulnerability exists in the Mac OS X version of Pixar Renderman 22.3.0's Install Helper helper tool. A user with local access can use this vulnerability to escalate their privileges to root. An attacker would need local access to the machine for a successful exploit. **CVE ID : CVE-2019-5015**	N/A	A-PIX-REND-040419/286

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
podofo_project					
podofo					
N/A	11-03-2019	7.5	PoDoFo 0.9.6 has a heap-based buffer overflow in PdfString::ConvertUTF16toUTF8 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 po-admin/route.php?mod=user&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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			urllib.parse.urlparse. The 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. **CVE ID : CVE-2019-9636**		
N/A	12-03-2019	4.3	An issue was discovered in 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**	N/A	A-PYT-PYTH-040419/290
quizandsurveymaster					
quiz_and_survey_master					
N/A	05-03-2019	4.3	The Quiz And Survey Master plugin 6.0.4 for WordPress allows wp-admin/admin.php?page=mlw_quiz_results quiz_id XSS. **CVE ID : CVE-2019-9575**	N/A	A-QUI-QUIZ-040419/291
rainbowpdf					
office_server_document_converter					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	07-03-2019	7.5	A heap overflow vulnerability exists in the PowerPoint document conversion function of Rainbow PDF Office Server Document Converter V7.0 Pro R1 (7,0,2018,1113). While parsing Document Summary Property Set stream, the getSummaryInformation function is incorrectly checking the correlation between size and the number of properties in PropertySet packets, causing an out-of-bounds write that leads to heap corruption and consequent code execution. **CVE ID : CVE-2019-5019**	N/A	A-RAI-OFFI-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-RED-SMAR-040419/293
RSA					
authentication_manager					
N/A	13-03-2019	4	RSA Authentication Manager versions prior to	N/A	A-RSA-AUTH-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_platform					
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. **CVE ID : CVE-2019-3824**	N/A	A-SAM-SAMB-040419/297
SAP					
businessobjects_business_intelligence					
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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Site Scripting (XSS) vulnerability. **CVE ID : CVE-2019-0269**		
advanced_business_application_programming_platform_kernel					
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-040419/300
advanced_business_application_programming_platform_krnl64nuc					
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	N/A	A-SAP-ADVA-040419/301

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_business_application_programming_platform_krnl64uc					
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_business_application_programming_platform_krnl32nuc					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-040419/303
advanced_business_application_programming_platform_krnl32uc					
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,	N/A	A-SAP-ADVA-040419/304

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. **CVE ID : CVE-2019-0270**		
advanced_business_application_programming_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 External 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**	N/A	A-SAP-ADVA-040419/305
sap_kernel					
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 External Entity (XEE) vulnerability. Fixed in Kernel 7.21 or 7.22, that is ABAP Server 7.00 to 7.31 and Kernel	N/A	A-SAP-SAP_-040419/306

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.45, 7.49 or 7.53, that is ABAP Server 7.40 to 7.52 or ABAP Platform. **CVE ID : CVE-2019-0271**		
mobile_platform_sdk					
N/A	12-03-2019	5	SAP Mobile Platform SDK allows an attacker to prevent legitimate users from accessing a service, either by crashing or flooding the service (i.e. denial of service). Fixed in versions 3.1 SP03 PL02, SDK 3.1 SP04, or later. **CVE ID : CVE-2019-0274**	N/A	A-SAP-MOBI-040419/307
netweaver_java_application_server					
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-040419/308
banking_services_from_sap					
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-040419/309

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inadequate authorization check for an authenticated user, potentially resulting in escalation of privileges. **CVE ID : CVE-2019-0276**		
s/4hana_financial_products_subledger					
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**	N/A	A-SAP-SFPS-040419/310
hana_extended_application_services					
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-040419/311
schoolcms					
schoolcms					
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

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-Type 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. **CVE ID : CVE-2019-9572**		
screen_stream_project					
screen_stream					
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. **CVE ID : CVE-2019-9833**	N/A	A-SCR-SCRE-040419/313
sdcms					
sdcms					
N/A	10-03-2019	7.5	An issue was discovered in SDCMS V1.7. In the \app\admin\controller\themecontroller.php file, the check_bad() function's filtering is not strict, resulting in PHP code execution. This occurs	N/A	A-SDC-SDCM-040419/314

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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=edit 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=User&a=add_post CSRF to add an admin account. **CVE ID : CVE-2019-9688**	N/A	A-SFT-SFTN-040419/316
shanda					
maplestory_online					
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 Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the IOCtl 0x8000c01c input value, leading to an integer signedness error and a heap-based buffer underflow. **CVE ID : CVE-2019-9729**		
Solarwinds					
orion_platform					
N/A	01-03-2019	7.5	SolarWinds Orion Platform before 2018.4 Hotfix 2 allows privilege escalation through the RabbitMQ service. **CVE ID : CVE-2019-9546**	https://support.solarwinds.com/Success_Center/Orion_Platform/Orion_Documentation/Additional_Resources/Orion_Platform_2018-4_Hotfix_2	A-SOL-ORIO-040419/318
spdk					
storage_performance_development_kit					
N/A	01-03-2019	5	In Storage Performance Development Kit (SPDK) before 19.01, a malicious vhost client (i.e., virtual machine) could carefully construct a circular descriptor chain that would result in a partial denial of service in the SPDK vhost target, because the vhost target did not properly detect such chains. **CVE ID : CVE-2019-9547**	https://github.com/spdk/spdk/releases/tag/v19.01	A-SPD-STOR-040419/319

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
stackstorm					
stackstorm					
N/A	08-03-2019	4.3	In st2web in StackStorm Web UI before 2.9.3 and 2.10.x before 2.10.3, it is possible to bypass the CORS protection mechanism via a "null" origin value, potentially leading to XSS. **CVE ID : CVE-2019-9580**	N/A	A-STA-STAC-040419/320
theolivetree					
ftp_server					
N/A	06-03-2019	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	14-03-2019	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	A-THI-CANA-040419/322

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Tibco					
jasperreports_server					
N/A	07-03-2019	4	The SOAP API component vulnerability of TIBCO Software Inc.'s TIBCO JasperReports Server, and TIBCO JasperReports Server for ActiveMatrix BPM contains a 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; 6.4.1; 6.4.2; 6.4.3, TIBCO JasperReports Server for ActiveMatrix BPM: versions up to and including 6.4.3. **CVE ID : CVE-2019-8986**	https://www.tibco.com/support/advisories/2019/03/tibco-security-advisory-march-6-2019-tibco-jasperreports-server-2018-8986	A-TIB-JASP-040419/323
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	A-TIN-TINY-040419/324

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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
N/A	13-03-2019	9.4	In tinysvcmdns through 2018-01-16, an mDNS server processing a crafted 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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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-2019-9748**		
treasuredata					
fluent_bit					
N/A	13-03-2019	5	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 packet, the plugin's mqtt_packet_drop function (in /plugins/in_mqtt/mqtt_prot.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.	N/A	A-TRE-FLUE-040419/327

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9749		
twinkletoessoftware					
booked					
N/A	05-03-2019	7.5	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/ManageThemePresenter.php does not ensure an image file extension. **CVE ID : CVE-2019-9581**	N/A	A-TWI-BOOK-040419/328
Vanillaforums					
vanilla_forums					
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+					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://support.apple.com/HT209451	A-WEB-WEBK-040419/331
Webmin					
Webmin					
N/A	07-03-2019	6.8	Webmin 1.900 allows remote attackers to execute arbitrary code by leveraging the "Java file manager" and "Upload and Download" privileges to upload a crafted .cgi file via the /updown/upload.cgi URI. **CVE ID : CVE-2019-9624**	N/A	A-WEB-WEBM-040419/332
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-WEB-LIBW-040419/333

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9746		
Wordpress					
Wordpress					
N/A	14-03-2019	6.8	WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated users in a default configuration. This occurs because CSRF protection is mishandled, and because Search Engine Optimization of A elements is performed incorrectly, leading to XSS. The XSS results in administrative access, which allows arbitrary changes to .php files. This is related to wp-admin/includes/ajax-actions.php and wp-includes/comment.php. **CVE ID : CVE-2019-9787**	N/A	A-WOR-WORD-040419/334
Yzmcms					
Yzmcms					
N/A	05-03-2019	3.5	An issue was discovered in YzmCMS 5.2.0. It has XSS via the bottom text field to the admin/system_manage/save.html URI, related to the site_code parameter. **CVE ID : CVE-2019-9570**	N/A	A-YZM-YZMC-040419/335
N/A	11-03-2019	3.5	Stored XSS exists in YzmCMS 5.2 via the admin/category/edit.html	N/A	A-YZM-YZMC-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"catname" parameter. **CVE ID : CVE-2019-9660**		040419/336
N/A	11-03-2019	3.5	Stored XSS exists in YzmCMS 5.2 via the admin/system_manage/user_config_edit.html "value" parameter, **CVE ID : CVE-2019-9661**	N/A	A-YZM-YZMC-040419/337
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

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. **CVE ID : CVE-2019-6215**	N/A	O-APP-TVOS-040419/340
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**	https://support.apple.com/HT209451	O-APP-TVOS-040419/341
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://support.apple.com/HT209451	O-APP-TVOS-040419/342

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2019-6217**		
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-TVOS-040419/343
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. **CVE ID : CVE-2019-6225**	N/A	O-APP-TVOS-040419/344
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-2019-6226**	https://support.apple.com/HT209451	O-APP-TVOS-040419/345
N/A	05-03-2019	6.8	A memory corruption	https://supp	O-APP-TVOS-

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
			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.com/HT209451	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://support.apple.com/HT209451	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://support.apple.com/HT209448	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://support.apple.com/HT209448	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://support.apple.com/HT209451	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://support.apple.com/HT209451	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://support.apple.com/HT209448	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://support.apple.com/HT209448	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	Description & CVE ID	Patch	NCIIPC ID
			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**		040419/355
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-WATC-040419/356
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	O-APP-WATC-040419/357
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	https://support.apple.com/HT209451	O-APP-WATC-040419/358

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for Windows, iCloud for Windows 7.10. Processing maliciously crafted web content may lead to arbitrary code execution. **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 arbitrary code execution. **CVE ID : CVE-2019-6217**	https://support.apple.com/HT209451	O-APP-WATC-040419/359
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, 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**	https://support.apple.com/HT209448	O-APP-WATC-040419/360
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-APP-WATC-040419/361

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			able to initiate a FaceTime call causing arbitrary code execution. **CVE ID : CVE-2019-6224**		
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-2019-6226**	https://support.apple.com/HT209451	O-APP-WATC-040419/362
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://support.apple.com/HT209451	O-APP-WATC-040419/363
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	https://support.apple.com/HT209448	O-APP-WATC-040419/364

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious application may be able to break out of its sandbox. **CVE ID : CVE-2019-6230**		
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://support.apple.com/HT209448	O-APP-WATC-040419/365
watch_os					
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://support.apple.com/HT209450	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://support.apple.com/HT209446	O-APP-IPHO-040419/367

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code. **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. **CVE ID : CVE-2019-6202**	https://support.apple.com/HT209448	O-APP-IPHO-040419/368
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-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**	https://support.apple.com/HT209443	O-APP-IPHO-040419/370
N/A	05-03-2019	4.3	A memory initialization issue was addressed with	N/A	O-APP-IPHO-040419/371

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://support.apple.com/HT209448	O-APP-IPHO-040419/373
N/A	05-03-2019	6.8	A memory corruption issue was addressed with improved state	https://support.apple.com/HT20944	O-APP-IPHO-040419/374

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management. 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. **CVE ID : CVE-2019-6211**	6	
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	O-APP-IPHO-040419/375
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-IPHO-040419/376
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	N/A	O-APP-IPHO-040419/377

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			may be able to break out of its sandbox. **CVE ID : CVE-2019-6214**		
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	O-APP-IPHO-040419/378
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**	https://support.apple.com/HT209451	O-APP-IPHO-040419/379
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://support.apple.com/HT209451	O-APP-IPHO-040419/380

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			maliciously crafted web content may lead to arbitrary code execution. **CVE ID : CVE-2019-6217**		
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-IPHO-040419/381
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, 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**	https://support.apple.com/HT209448	O-APP-IPHO-040419/382
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://support.apple.com/HT209450	O-APP-IPHO-040419/383
N/A	05-03-2019	5	A logic issue existed in the	https://supp	O-APP-IPHO-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 answer. **CVE ID : CVE-2019-6223**	ort.apple.com/HT209521	040419/384
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-IPHO-040419/385
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. **CVE ID : CVE-2019-6225**	N/A	O-APP-IPHO-040419/386
N/A	05-03-2019	6.8	Multiple memory corruption issues were addressed with improved	https://support.apple.com/HT20945	O-APP-IPHO-040419/387

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	1	
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://support.apple.com/HT209451	O-APP-IPHO-040419/388
N/A	05-03-2019	4.3	A cross-site scripting issue existed in Safari. This issue was addressed with improved URL validation. 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**	https://support.apple.com/HT209449	O-APP-IPHO-040419/389
N/A	05-03-2019	4.3	A logic issue was addressed with improved validation. This issue is	https://support.apple.com/HT20945	O-APP-IPHO-040419/390

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	1	
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://support.apple.com/HT209448	O-APP-IPHO-040419/391
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://support.apple.com/HT209448	O-APP-IPHO-040419/392
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,	https://support.apple.com/HT209451	O-APP-IPHO-040419/393

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://support.apple.com/HT209451	O-APP-IPHO-040419/394
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://support.apple.com/HT209450	O-APP-IPHO-040419/395
mac_os_x					
N/A	05-03-2019	5.8	An out-of-bounds read was addressed with improved input validation. This issue	https://support.apple.com/HT20944	O-APP-MAC_-040419/396

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is 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. **CVE ID : CVE-2019-6200**	6	
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://support.apple.com/HT209448	O-APP-MAC_-040419/397
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-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 (CVSS)	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-MAC_-040419/400
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://support.apple.com/HT209448	O-APP-MAC_-040419/401
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://support.apple.com/HT209446	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://support.apple.com/HT209448	O-APP-MAC_-040419/406

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://support.apple.com/HT209446	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://support.apple.com/HT209450	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://support.apple.com/HT209521	O-APP-MAC_-040419/409

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-6225**	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://support.apple.com/HT209448	O-APP-MAC_-040419/412
N/A	05-03-2019	4.3	An out-of-bounds read was addressed with improved	https://support.apple.co	O-APP-MAC_-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	m/HT209448	040419/413
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://support.apple.com/HT209450	O-APP-MAC_-040419/414
broadcastboxes					
scion-8_firmware					
N/A	15-03-2019	5	CircuitWerkes Sicon-8, a hardware device used for managing electrical devices, ships with a web-based 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**	N/A	O-BRO-SCIO-040419/415
Canonical					
ubuntu_linux					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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. **CVE ID : CVE-2019-3824**	N/A	O-CAN-UBUN-040419/416
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	O-CAN-UBUN-040419/417
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	O-CAN-UBUN-040419/418

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Carel					
pcoweb_card_firmware					
N/A	01-03-2019	5	The Glen Dimplex Deutschland GmbH implementation of the Carel pCOWeb configuration tool allows remote attackers to obtain access via an HTTP session on port 10000, as demonstrated by reading the modem password (which is 1234), or reconfiguring "party mode" or "vacation mode." **CVE ID : CVE-2019-9484**	N/A	O-CAR-PCOW-040419/419
chuango					
a11_pstn/lcd/rfid_touch_alarm_system_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-A11_-040419/420
a8_pstn_alarm_system_firmware					
N/A	11-03-2019	6.4	The Chuango 433 MHz burglar-alarm product line	N/A	O-CHU-A8_P-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			uses 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 Wifi Alarm System. **CVE ID : CVE-2019-9659**		040419/421
awv_plus_wifi_alarm_system_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-AWV_-040419/422
b11_dual-network_alarm_system_firmware					
N/A	11-03-2019	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-B11_-040419/423

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
cg-105s_on-site_alarm_system_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-CG-1-040419/424
g3_gsm/sms_alarm_system_firmware					
N/A	11-03-2019	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 attacks, as demonstrated by Chuango branded products, and non-Chuango branded products such as the	N/A	O-CHU-G3_G-040419/425

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Eminent EM8617 OV2 Wifi Alarm System. **CVE ID : CVE-2019-9659**		
g5_plus_gsm/sms/rfid_touch_alarm_system_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-G5_P-040419/426
g5w_3g_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-G5W_-040419/427
Wifi/cellular_smart_home_system_h4_plus_firmware					

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	11-03-2019	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 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**	N/A	O-CHU-WIFI-040419/428
wifi_alarm_system_firmware					
N/A	11-03-2019	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 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**	N/A	O-CHU-WIFI-040419/429
Cisco					
Nx-os					
N/A	06-03-2019	7.2	A vulnerability in the controller authorization functionality of Cisco	N/A	O-CIS-NX-O-040419/430

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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation checking mechanisms of user-supplied 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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	O-CIS-NX-O-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**		

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 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	N/A	O-CIS-NX-O-040419/438

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	O-CIS-NX-O-040419/439

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could cause the network stack of an affected device to run out of available buffers, impairing operations of control plane and management plane protocols, resulting in a DoS condition. Note: This vulnerability can be triggered only by traffic that is destined to an affected device and cannot be exploited using traffic that transits an affected device. Nexus 1000V Switch for Microsoft Hyper-V is affected in versions prior to 5.2(1)SM3(2.1). Nexus 1000V Switch for VMware vSphere is affected in versions prior to 5.2(1)SV3(4.1a). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I7(6) and 9.2(2). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(11), 7.0(3)I7(6), and 9.2(2). Nexus 3600 Platform Switches are affected in versions prior to 7.0(3)F3(5) and 9.2(2). Nexus 5500, 5600, and 6000 Series Switches are affected in versions prior to 7.1(5)N1(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): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of Service; XSS- Cross Site Scripting; Sql- SQL Injection; N/A- Not Applicable.

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.3(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). **CVE ID : CVE-2019-1599**		
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 Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4100 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. Firepower 9300 Series Next-Generation Firewalls are affected in versions prior to 2.2.2.91 and 2.3.1.110. MDS 9000 Series Multilayer Switches are affected in versions prior to 6.2(25), 8.1(1b), and 8.3(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600 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		

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Fabric Modules are affected in versions prior to 7.0(3)F3(5). **CVE ID : CVE-2019-1600**		
N/A	08-03-2019	7.2	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 Switches are affected in versions prior to 7.0(3)I4(9) and 7.0(3)I7(4). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(10) and 7.0(3)I7(4). Nexus 3600	N/A	O-CIS-NX-O-040419/441

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2019-1604**		
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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code as root. The vulnerability is due to incorrect input validation in the NX-API feature. An attacker could exploit this vulnerability by sending a crafted HTTP or HTTPS request to an internal service on an affected device that has the NX-API feature enabled. A successful exploit could allow the attacker to cause a buffer overflow and execute arbitrary code as root. Note: The NX-API feature is disabled by default. MDS 9000 Series Multilayer Switches are affected in versions prior to 8.1(1). Nexus 3000 Series Switches are affected in versions prior to 7.0(3)I4(8) and 7.0(3)I7(1). Nexus 3500 Platform Switches are affected in versions prior to 6.0(2)A8(8). Nexus 3600 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 7.3(2)N1(1). Nexus 7000 and 7700 Series Switches are affected in versions prior to 7.3(3)D1(1). Nexus		

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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. 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
			are affected in versions prior to 6.2(22), 7.3(3)D1(1), and 8.2(3). **CVE ID : CVE-2019-1608**		
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. 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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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)I7(4) are affected. **CVE ID : CVE-2019-1610**		
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 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. Firepower 4100 Series Next-Generation Firewalls are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. Firepower 9300 Security Appliance are affected running software versions prior to 2.2.2.91, 2.3.1.110, and 2.4.1.222. MDS 9000 Series Multilayer Switches are affected running software versions prior to 6.2(25) and 8.3(1). Nexus 3000 Series Switches are affected running software versions prior to 7.0(3)I4(9) and 7.0(3)I7(5). Nexus 3500 Platform Switches are affected running software versions prior to 7.0(3)I7(5). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 2000, 5500, 5600, and 6000 Series Switches are		

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected 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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 running software versions prior to 6.2(27) 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(6). Nexus 3500 Platform Switches are affected running software versions prior to 6.0(2)A8(11) and 7.0(3)I7(6). Nexus 3600 Platform Switches are affected running software versions prior to 7.0(3)F3(5). Nexus 9000 Series Switches in Standalone NX-OS Mode are affected running		

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)	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
			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).		

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)I4(9) and 7.0(3)I7(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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7.0(3)I7(4). Nexus 3600 Platform Switches 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). 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 9500 R-Series Line Cards and Fabric Modules are affected running software versions prior to 7.0(3)F3(5). UCS 6200, 6300, and 6400 Fabric Interconnects are affected running software versions prior to 3.2(3j) and 4.0(2a). **CVE ID : CVE-2019-1616**		
application_policy_infrastructure_controller_software					
N/A	06-03-2019	7.2	A vulnerability in the controller authorization functionality of Cisco 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	N/A	O-CIS-APPL-040419/455

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
Debian					
debian_linux					
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. **CVE ID : CVE-2019-3824**	N/A	O-DEB-DEBI-040419/456
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	N/A	O-DEB-DEBI-040419/457

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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	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_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len. **CVE ID : CVE-2019-9638**	N/A	O-DEB-DEBI-040419/458
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	O-DEB-DEBI-040419/459
eminent					
em8617_ov2_wifi_alarm_system_firmware					
N/A	11-03-2019	6.4	The Chuango 433 MHz burglar-alarm product line uses static codes in the RF	N/A	O-EMI-EM86-040419/460

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_firmware					
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_firmware					
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

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_5601f_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					
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

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-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0595**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0595	O-MIC-WIND-040419/466
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-040419/468

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0598	O-MIC-WIND-040419/469
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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/470

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. **CVE ID : CVE-2019-0600**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/473

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618	O-MIC-WIND-040419/476

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0616, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/477
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0623	O-MIC-WIND-040419/479

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-2019-0597, CVE-2019-0598, CVE-2019-0599. **CVE ID : CVE-2019-0625**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/480
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0626	O-MIC-WIND-040419/481
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0627	O-MIC-WIND-040419/482
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when	https://portal.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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0628**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0628	040419/483
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0630	O-MIC-WIND-040419/484
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0631	O-MIC-WIND-040419/485
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0632	O-MIC-WIND-040419/486

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0627, CVE-2019-0631. **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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/487
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0635	O-MIC-WIND-040419/488
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0636	O-MIC-WIND-040419/489
N/A	05-03-2019	5	A security feature bypass vulnerability exists when Windows Defender	https://portal.msrc.microsoft.com/en	O-MIC-WIND-040419/490

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/493

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/494
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/495
windows_7					
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0595	O-MIC-WIND-040419/496

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0596	O-MIC-WIND-040419/497
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0597	O-MIC-WIND-040419/498
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when	https://portal.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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the 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**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0598	040419/499
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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/500
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0600	O-MIC-WIND-040419/501

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0619, CVE-2019-0660,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/504

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0664. **CVE ID : CVE-2019-0615**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0616	O-MIC-WIND-040419/505
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-2019-0662. **CVE ID : CVE-2019-0618**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618	O-MIC-WIND-040419/506
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/507

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0597, CVE-2019-0598, CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/510

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0628	O-MIC-WIND-040419/512
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-040419/514

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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**	guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0635	O-MIC-WIND-040419/515
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0636	O-MIC-WIND-040419/516
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-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/517

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0616, CVE-2019-0619, CVE-2019-0664. **CVE ID : CVE-2019-0660**		
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. **CVE ID : CVE-2019-0661**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0661	O-MIC-WIND-040419/518
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/519
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/520

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is 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. **CVE ID : CVE-2019-0664**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0664	O-MIC-WIND-040419/521
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. **CVE ID : CVE-2019-5921**	N/A	O-MIC-WIND-040419/522
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0595	O-MIC-WIND-040419/523

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0599, CVE-2019-0625. **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-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0596**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0596	O-MIC-WIND-040419/524
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0597	O-MIC-WIND-040419/525
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/526

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	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-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625. **CVE ID : CVE-2019-0599**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/527
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0600	O-MIC-WIND-040419/528
N/A	05-03-2019	1.9	An information disclosure vulnerability exists when the Human Interface Devices (HID) component	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-040419/529

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly handles objects in memory, aka 'HID Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0600. **CVE ID : CVE-2019-0601**	guidance/advisory/CVE-2019-0601	
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/530
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/531
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when	https://portal.msrc.micr	O-MIC-WIND-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0616	040419/532
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-2019-0662. **CVE ID : CVE-2019-0618**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618	O-MIC-WIND-040419/533
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-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/534

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0621	O-MIC-WIND-040419/535
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0623	O-MIC-WIND-040419/536
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/537
N/A	05-03-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP	https://portal.msrc.microsoft.com/en	O-MIC-WIND-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	-US/security-guidance/advisory/CVE-2019-0626	040419/538
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0628	O-MIC-WIND-040419/539
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0630	O-MIC-WIND-040419/540
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-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/541

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0656	O-MIC-WIND-040419/544
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/545

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This 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**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/546
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/547
N/A	05-03-2019	4.3	An information disclosure vulnerability exists when the Windows GDI component improperly discloses the contents of	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-040419/548

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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. **CVE ID : CVE-2019-0664**	visory/CVE-2019-0664	
windows_rt_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-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0595**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0595	O-MIC-WIND-040419/549
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.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0596	O-MIC-WIND-040419/550

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0596		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/553

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2019-0595, CVE-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625. **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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0600	O-MIC-WIND-040419/554
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0601	O-MIC-WIND-040419/555
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/556

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/557
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0616	O-MIC-WIND-040419/558
N/A	05-03-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-040419/559

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥	(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**	guidance/advisory/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-2019-0616, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/560
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0621	O-MIC-WIND-040419/561
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	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-040419/562

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0628	O-MIC-WIND-040419/565

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0630	O-MIC-WIND-040419/566
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/567
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0636	O-MIC-WIND-040419/568
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/569

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2019-0656**	2019-0656	
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/570
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/571
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/572

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. **CVE ID : CVE-2019-0664**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0664	O-MIC-WIND-040419/573
windows_server_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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0595	O-MIC-WIND-040419/574
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when	https://portal.msrc.micr	O-MIC-WIND-

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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0598	O-MIC-WIND-040419/577

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0596, CVE-2019-0597, CVE-2019-0598, CVE-2019-0625. **CVE ID : CVE-2019-0599**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0601	O-MIC-WIND-040419/580

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0600. **CVE ID : CVE-2019-0601**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/581
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/582
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/583

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0602, CVE-2019-0615, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	2019-0616	
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-2019-0662. **CVE ID : CVE-2019-0618**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618	O-MIC-WIND-040419/584
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-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/585
N/A	05-03-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-040419/586

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0661, CVE-2019-0663. **CVE ID : CVE-2019-0621**	visory/CVE-2019-0621	
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0623	O-MIC-WIND-040419/587
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/588
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0626	O-MIC-WIND-040419/589

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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. **CVE ID : CVE-2019-0630**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/592
N/A	05-03-2019	5.5	An information disclosure vulnerability exists when	https://portal.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

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
			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**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0635	040419/593
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0636	O-MIC-WIND-040419/594
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/595
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/596

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0621, CVE-2019-0663. **CVE ID : CVE-2019-0661**	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/597
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/598
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/599

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-2019-0619, CVE-2019-0660. **CVE ID : CVE-2019-0664**	2019-0664	
windows_server_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-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0595**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0596**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0596	O-MIC-WIND-040419/601

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/604

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-2019-0599**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0600	O-MIC-WIND-040419/605
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0601	O-MIC-WIND-040419/606
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-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/607

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/608
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0616	O-MIC-WIND-040419/609
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	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-040419/610

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the memory, aka 'GDI+ Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0662. **CVE ID : CVE-2019-0618**	visory/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-2019-0616, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0619	O-MIC-WIND-040419/611
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0621	O-MIC-WIND-040419/612
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/613

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0623**	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/614
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0626	O-MIC-WIND-040419/615
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0628	O-MIC-WIND-040419/616
N/A	05-03-2019	9	A remote code execution	https://port	O-MIC-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0630	WIND-040419/617
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/618
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0635	O-MIC-WIND-040419/619
N/A	05-03-2019	2.1	An information vulnerability exists when Windows improperly	https://portal.msrc.microsoft.com/en	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

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
			discloses file information, aka 'Windows Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0636**	-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0661	O-MIC-WIND-040419/623

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟩	**CVE ID : CVE-2019-0661**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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): 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
			2019-0615, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660. **CVE ID : CVE-2019-0664**		
windows_server_2016					
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en	O-MIC-WIND-040419/629

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/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0597, CVE-2019-0598, CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0599	O-MIC-WIND-040419/631

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		🟥	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0619, CVE-2019-0660,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/634

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0664. **CVE ID : CVE-2019-0602**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/635
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0616	O-MIC-WIND-040419/636
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/637

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-2019-0616, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0619**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0623	O-MIC-WIND-040419/640

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/641
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0626	O-MIC-WIND-040419/642
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.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0628	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-040419/647

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass Device Guard, aka 'Windows Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0627, CVE-2019-0631. **CVE ID : CVE-2019-0632**	guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/650

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0636	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'. **CVE ID : CVE-2019-0637**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0637	O-MIC-WIND-040419/651
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/654

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/655
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0663	O-MIC-WIND-040419/656
windows_server_2019					
N/A	05-03-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database	https://portal.msrc.microsoft.com/en	O-MIC-WIND-040419/657

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	-US/security-guidance/advisory/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-2019-0597, CVE-2019-0598, CVE-2019-0599, CVE-2019-0625. **CVE ID : CVE-2019-0596**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-2019-0598, CVE-2019-0599, CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0597	O-MIC-WIND-040419/659

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0625. **CVE ID : 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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0598	O-MIC-WIND-040419/660
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**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-040419/662

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0601. **CVE ID : CVE-2019-0600**	2019-0600	
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0601	O-MIC-WIND-040419/663
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0602**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0602	O-MIC-WIND-040419/664
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0615	O-MIC-WIND-040419/665

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This CVE ID is unique from CVE-2019-0602, CVE-2019-0616, CVE-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0615**		
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-2019-0619, CVE-2019-0660, CVE-2019-0664. **CVE ID : CVE-2019-0616**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0616	O-MIC-WIND-040419/666
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-2019-0662. **CVE ID : CVE-2019-0618**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0618	O-MIC-WIND-040419/667
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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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-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
			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**	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0621	O-MIC-WIND-040419/669
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0625	O-MIC-WIND-040419/670
N/A	05-03-2019	7.5	A memory corruption vulnerability exists in the Windows Server DHCP service when an attacker	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-040419/671

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sends specially crafted packets to a DHCP server, aka 'Windows DHCP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0626**	guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0631	O-MIC-WIND-040419/675
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. **CVE ID : CVE-2019-0632**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0632	O-MIC-WIND-040419/676
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0633	O-MIC-WIND-040419/677
N/A	05-03-2019	5.5	An information disclosure	https://port	O-MIC-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0656	O-MIC-WIND-040419/681

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0659	O-MIC-WIND-040419/682
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0660	O-MIC-WIND-040419/683
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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0662	O-MIC-WIND-040419/684
Motorola					
c1_firmware					
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 SetNetworkTomographySettings 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 SetNetworkTomographySettings API function, as demonstrated by shell metacharacters in the tomography_ping_number field.	N/A	O-MOT-M2_F-040419/690

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-9117		
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 SetNTPServerSettings API function, as demonstrated by shell metacharacters in the system_time_timezone field. **CVE ID : CVE-2019-9118**	N/A	O-MOT-M2_F-040419/691
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-MOT-M2_F-040419/692

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)	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 SetSmartQoSSettings API function, as demonstrated by shell metacharacters in the smartqos_priority_devices field. **CVE ID : CVE-2019-9121**		M2_F-040419/694
Moxa					
eds-405a_firmware					
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. **CVE ID : CVE-2019-6518**	N/A	O-MOX-EDS--040419/695
N/A	05-03-2019	5	Moxa IKS and EDS does not properly check authority on server side,	N/A	O-MOX-EDS--040419/696

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which results in a read-only user being able to perform arbitrary configuration changes. **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. **CVE ID : CVE-2019-6522**	N/A	O-MOX-EDS--040419/697
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--040419/698
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--040419/699
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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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_firmware					
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

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 read-only 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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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 cause the switch to crash. **CVE ID : CVE-2019-6559**	N/A	O-MOX-EDS--040419/709
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	O-MOX-EDS--040419/710
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	O-MOX-EDS--040419/712
eds-510a_firmware					
N/A	05-03-2019	5	Moxa IKS and EDS store plaintext passwords,	N/A	O-MOX-EDS--

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. **CVE ID : CVE-2019-6518**		040419/713
N/A	05-03-2019	5	Moxa IKS and EDS does not properly check authority on server side, which results in a read-only user being able to perform arbitrary configuration changes. **CVE ID : CVE-2019-6520**	N/A	O-MOX-EDS--040419/714
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--040419/715
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	Description & CVE ID	Patch	NCIIPC ID
			EDS, which may allow remote code execution. **CVE ID : CVE-2019-6557**		
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 cause the switch to crash. **CVE ID : CVE-2019-6559**	N/A	O-MOX-EDS--040419/718
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--040419/719
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--040419/720
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**	N/A	O-MOX-EDS--040419/721

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
iks-g6824a_firmware					
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. **CVE ID : CVE-2019-6518**	N/A	O-MOX-IKS--040419/722
N/A	05-03-2019	5	Moxa IKS and EDS does not properly check authority on server side, which results in a read-only user being able to perform arbitrary configuration changes. **CVE ID : CVE-2019-6520**	N/A	O-MOX-IKS--040419/723
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-IKS--040419/724
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-IKS--040419/725

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	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-IKS--040419/726
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 cause the switch to crash. **CVE ID : CVE-2019-6559**	N/A	O-MOX-IKS--040419/727
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-IKS--040419/728
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-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

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used to send a malicious script. **CVE ID : CVE-2019-6565**		
Nokia					
i-240w-q_gpon_ont_firmware					
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. **CVE ID : CVE-2019-3918**	N/A	O-NOK-I-24-040419/732
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_Form?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	O-NOK-I-24-040419/734

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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?script/. 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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			this vulnerability to potentially execute arbitrary code. **CVE ID : CVE-2019-3922**		
psigridconnect					
iec104_security_proxy_firmware					
N/A	05-03-2019	6.5	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**	N/A	O-PSI-IEC1-040419/737
Sagemcom					
f@st_5260_firmware					
N/A	05-03-2019	5	Sagemcom F@st 5260 routers using firmware	N/A	O-SAG-F@ST-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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\x06\x43\x01\x00\xac\xff\x00 (aka UID 0x43) requests to TCP port 502. **CVE ID : CVE-2019-9590**	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	O-ZYX-NBG--040419/740