National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Apr 2019 Vol. 06 No. 07

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
74cms					
74cms					
Improper Control of Generation of Code ('Code Injection')	01-04-2019	7.5	Application/Admin/Controller/ConfigController.class.php in 74cms v5.0.1 allows remote attackers to execute arbitrary PHP code via the index.php?m=Admin&c=config&a=edit site_domain parameter. **CVE ID : CVE-2019-10684**	N/A	A-74C-74CM-010519/1
Advantech					
webaccess					
Unrestricted Upload of File with Dangerous Type	09-04-2019	7.5	Advantech WebAccess 8.3.4 is vulnerable to file upload attacks via unauthenticated RPC call. An unauthenticated, remote attacker can use this vulnerability to execute arbitrary code. **CVE ID : CVE-2019-3940**	N/A	A-ADV-WEBA-010519/2
Improper Access Control	09-04-2019	6.4	Advantech WebAccess 8.3.4 allows unauthenticated, remote attackers to delete arbitrary files via IOCTL 10005 RPC. **CVE ID : CVE-2019-3941**	N/A	A-ADV-WEBA-010519/3

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	05-04-2019	7.5	Advantech WebAccess/SCADA, Versions 8.3.5 and prior. Multiple stack-based buffer overflow vulnerabilities, caused by a lack of proper validation of the length of user-supplied data, may allow remote code execution. **CVE ID : CVE-2019-6550**	N/A	A-ADV-WEBA-010519/4
Improper Neutralization of Special Elements used in a Command ('Command Injection')	05-04-2019	7.5	Advantech WebAccess/SCADA, Versions 8.3.5 and prior. Multiple command injection vulnerabilities, caused by a lack of proper validation of user-supplied data, may allow remote code execution. **CVE ID : CVE-2019-6552**	N/A	A-ADV-WEBA-010519/5
Improper Access Control	05-04-2019	5	Advantech WebAccess/SCADA, Versions 8.3.5 and prior. An improper access control vulnerability may allow an attacker to cause a denial-of-service condition. **CVE ID : CVE-2019-6554**	N/A	A-ADV-WEBA-010519/6
airsonic_project					
airsonic					
N/A	07-04-2019	5	Airsonic 10.2.1 uses Spring's default remember-me mechanism based on MD5, with a fixed	N/A	A-AIR-AIRS-010519/7

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			key of airsonic in GlobalSecurityConfig.java. An attacker able to capture cookies might be able to trivially bruteforce offline the passwords of associated users. **CVE ID : CVE-2019-10907**		
N/A	07-04-2019	7.5	In Airsonic 10.2.1, RecoverController.java generates passwords via org.apache.commons.lang. RandomStringUtils, which uses java.util.Random internally. This PRNG has a 48-bit seed that can easily be bruteforced, leading to trivial privilege escalation attacks. **CVE ID : CVE-2019-10908**	N/A	A-AIR-AIRS-010519/8
Apache					
tomcat					
Uncontrolled Resource Consumption	10-04-2019	5	The HTTP/2 implementation in Apache Tomcat 9.0.0.M1 to 9.0.14 and 8.5.0 to 8.5.37 accepted streams with excessive numbers of SETTINGS frames and also permitted clients to keep streams open without reading/writing request/response data. By keeping streams open for requests that utilised the Servlet API's blocking I/O, clients were able to cause	https://security.netapp.com/advisory/ntap-20190419-0001/	A-APA-TOMC-010519/9

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server-side threads to block eventually leading to thread exhaustion and a DoS. **CVE ID : CVE-2019-0199**		
Improper Input Validation	15-04-2019	9.3	When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassages	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-784	A-APA-TOMC-010519/10

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/). **CVE ID : CVE-2019-0232**		
airflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-04-2019	3.5	A malicious admin user could edit the state of objects in the Airflow metadata database to execute arbitrary javascript on certain page views. **CVE ID : CVE-2019-0216**	N/A	A-APA-AIRF-010519/11
Cross-Site Request Forgery (CSRF)	10-04-2019	6.8	A number of HTTP endpoints in the Airflow webserver (both RBAC and classic) did not have adequate protection and were vulnerable to cross-site request forgery attacks. **CVE ID : CVE-2019-0229**	N/A	A-APA-AIRF-010519/12
http_server					
N/A	08-04-2019	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by	N/A	A-APA-HTTP-010519/13

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			manipulating the scoreboard. Non-Unix systems are not affected. **CVE ID : CVE-2019-0211**		
Improper Access Control	08-04-2019	6	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions. **CVE ID : CVE-2019-0215**	N/A	A-APA-HTTP-010519/14
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**	N/A	A-APA-HTTP-010519/15
Autodesk					
advance_steel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD	N/A	A-AUT-ADVA-010519/16

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution.	N/A	A-AUT-ADVA-010519/17

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
			CVE ID : CVE-2019-7359		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**	N/A	A-AUT-ADVA-010519/18
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD	N/A	A-AUT-ADVA-010519/19

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**		
autocad					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting	N/A	A-AUT-AUTO-010519/20

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**	N/A	A-AUT-AUTO-010519/21
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018,	N/A	A-AUT-AUTO-010519/22

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil	N/A	A-AUT-AUTO-010519/23

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3D 2018. **CVE ID : CVE-2019-7361**		
autocad_architecture					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**	N/A	A-AUT-AUTO-010519/24
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk	N/A	A-AUT-AUTO-010519/25

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
			AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may	N/A	A-AUT-AUTO-010519/26

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**	N/A	A-AUT-AUTO-010519/27
autocad_electrical					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/28

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution.	N/A	A-AUT-AUTO-010519/29

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-7359		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**	N/A	A-AUT-AUTO-010519/30
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/31

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**		
autocad_lt					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting	N/A	A-AUT-AUTO-010519/32

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**	N/A	A-AUT-AUTO-010519/33
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018,	N/A	A-AUT-AUTO-010519/34

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil	N/A	A-AUT-AUTO-010519/35

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3D 2018. **CVE ID : CVE-2019-7361**		
autocad_map_3d					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**	N/A	A-AUT-AUTO-010519/36
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk	N/A	A-AUT-AUTO-010519/37

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
			AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may	N/A	A-AUT-AUTO-010519/38

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**	N/A	A-AUT-AUTO-010519/39
autocad_mechanical					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/40

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution.	N/A	A-AUT-AUTO-010519/41

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-7359		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**	N/A	A-AUT-AUTO-010519/42
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/43

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**		
autocad_mep					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting	N/A	A-AUT-AUTO-010519/44

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**	N/A	A-AUT-AUTO-010519/45
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018,	N/A	A-AUT-AUTO-010519/46

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
			Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil	N/A	A-AUT-AUTO-010519/47

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3D 2018. **CVE ID : CVE-2019-7361**		
autocad_p&id					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**	N/A	A-AUT-AUTO-010519/48
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk	N/A	A-AUT-AUTO-010519/49

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may	N/A	A-AUT-AUTO-010519/50

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**	N/A	A-AUT-AUTO-010519/51
autocad_plant_3d					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/52

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
			Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution.	N/A	A-AUT-AUTO-010519/53

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-7359		
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**	N/A	A-AUT-AUTO-010519/54
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD	N/A	A-AUT-AUTO-010519/55

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. **CVE ID : CVE-2019-7361**		
civil_3d					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting	N/A	A-AUT-CIVI-010519/56

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in code execution. **CVE ID : CVE-2019-7358**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7359**	N/A	A-AUT-CIVI-010519/57
Use After Free	09-04-2019	6.8	An exploitable heap overflow vulnerability in the DXF-parsing functionality in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018,	N/A	A-AUT-CIVI-010519/58

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil 3D 2018. A specially crafted DXF file with too many cell margins populating an AcCellMargin object may cause a heap overflow, resulting in code execution. **CVE ID : CVE-2019-7360**		
Deserialization of Untrusted Data	09-04-2019	6.8	An attacker may convince a victim to open a malicious action micro (.actm) file that has serialized data, which may trigger a code execution in Autodesk Advance Steel 2018, Autodesk AutoCAD 2018, Autodesk AutoCAD Architecture 2018, Autodesk AutoCAD Electrical 2018, Autodesk AutoCAD Map 3D 2018, Autodesk AutoCAD Mechanical 2018, Autodesk AutoCAD MEP 2018, Autodesk AutoCAD P&ID 2018, Autodesk AutoCAD Plant 3D 2018, Autodesk AutoCAD LT 2018, and Autodesk Civil	N/A	A-AUT-CIVI-010519/59

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3D 2018. **CVE ID : CVE-2019-7361**		
aveva					
wonderware_system_platform					
N/A	11-04-2019	4	AVEVA Wonderware System Platform 2017 Update 2 and prior uses an ArchestrA network user account for authentication of system processes and inter-node communications. A user with low privileges could make use of an API to obtain the credentials for this account. **CVE ID : CVE-2019-6525**	https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec135.pdf	A-AVE-WOND-010519/60
Bolt					
bolt					
Cross-Site Request Forgery (CSRF)	05-04-2019	6.8	Cross Site Request Forgery (CSRF) in the bolt/upload File Upload feature in Bolt CMS 3.6.6 allows remote attackers to execute arbitrary code by uploading a JavaScript file to include executable extensions in the file/edit/config/config.yml configuration file. **CVE ID : CVE-2019-10874**	N/A	A-BOL-BOLT-010519/61
buttle_project					
buttle					
Improper Neutralizatio	03-04-2019	4.3	XSS in buttle npm package version 0.2.0 causes	N/A	A-BUT-BUTT-

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 of Input During Web Page Generation ('Cross-site Scripting')			execution of attacker-provided code in the victim's browser when an attacker creates an arbitrary file on the server. **CVE ID : CVE-2019-5422**		010519/62
Cacti					
cacti					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	3.5	In clearFilter() in utilities.php in Cacti before 1.2.3, no escaping occurs before printing out the value of the SNMP community string (SNMP Options) in the View poller cache, leading to XSS. **CVE ID : CVE-2019-11025**	N/A	A-CAC-CACT-010519/63
cantemo					
portal					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-04-2019	6	Cantemo Portal before 3.2.13, 3.3.x before 3.3.8, and 3.4.x before 3.4.9 has XSS. Leveraging this vulnerability would enable performing actions as users, including administrative users. This could enable account creation and deletion as well as deletion of information contained within the app. **CVE ID : CVE-2019-7551**	N/A	A-CAN-PORT-010519/64
Checkpoint					
ipsec_vpn					

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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	09-04-2019	4.3	Check Point IKEv2 IPsec VPN up to R80.30, in some less common conditions, may allow an attacker with knowledge of the internal configuration and setup to successfully connect to a site-to-site VPN server. **CVE ID : CVE-2019-8456**	N/A	A-CHE-IPSE-010519/65
Clamav					
clamav					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-04-2019	6.8	A vulnerability in the RAR file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and 0.101.0 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper error-handling mechanisms when processing nested RAR files sent to an affected device. An attacker could exploit this vulnerability by sending a crafted RAR file to an affected device. An exploit could allow the attacker to view or create arbitrary files on the targeted system. **CVE ID : CVE-2019-1785**	N/A	A-CLA-CLAM-010519/66

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	08-04-2019	4.3	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and 0.101.0 could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1786**	N/A	A-CLA-CLAM-010519/67
Out-of-bounds Read	08-04-2019	4.3	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial	N/A	A-CLA-CLAM-010519/68

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause a heap buffer out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1787**		
Improper Input Validation	08-04-2019	4.3	A vulnerability in the Object Linking & Embedding (OLE2) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for OLE2 files sent an affected device. An attacker could exploit this	N/A	A-CLA-CLAM-010519/69

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
			vulnerability by sending malformed OLE2 files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds write condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1788**		
Out-of-bounds Read	08-04-2019	4.3	A vulnerability in the Portable Executable (PE) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for PE files sent an affected device. An attacker could exploit this vulnerability by sending malformed PE files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds read condition, resulting in a crash that could result in a denial of	N/A	A-CLA-CLAM-010519/70

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service condition on an affected device. **CVE ID : CVE-2019-1798**		
Claws-mail					
mail					
Inadequate Encryption Strength	07-04-2019	4.3	In Claws Mail 3.14.1, an attacker in possession of S/MIME or PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, they unknowingly leak the plaintext of the encrypted message part(s) back to the attacker. **CVE ID : CVE-2019-10735**	N/A	A-CLA-MAIL-010519/71
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	11-04-2019	6.5	An issue was discovered in CMS Made Simple 2.2.8. In the module FrontEndUsers (in the file class.FrontEndUsersManipulate.php or class.FrontEndUsersManipulator.php), it is possible	https://www.cmsmadesimple.org/2019/03/Announcing-CMS-Made-Simple-v2.2.10-	A-CMS-CMS_-010519/72

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			to reach an unserialize call with an untrusted __FEU__ cookie, and achieve authenticated object injection. **CVE ID : CVE-2019-9056**	Spuzzum	
ctolog					
thinkadmin					
N/A	08-04-2019	5	application\admin\controller\User.php in ThinkAdmin V4.0 does not prevent continued use of an administrator's cookie-based credentials after a password change. **CVE ID : CVE-2019-11018**	N/A	A-CTO-THIN-010519/73
ctrip					
apollo					
Server-Side Request Forgery (SSRF)	01-04-2019	7.5	An SSRF vulnerability was found in an API from Ctrip Apollo through 1.4.0-SNAPSHOT. An attacker may use it to do an intranet port scan or raise a GET request via /system-info/health because the %23 substring is mishandled. **CVE ID : CVE-2019-10686**	N/A	A-CTR-APOL-010519/74
Eclipse					
hawkbit					
N/A	03-04-2019	6.8	Eclipse hawkBit versions prior to 0.3.0M2 resolved Maven build artifacts for the Vaadin based UI over	https://bugs.eclipse.org/bugs/show_bug.cgi?id=546	A-ECL-HAWK-010519/75

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP instead of HTTPS. Any of these dependent artifacts could have been maliciously compromised by a MITM attack. Hence produced build artifacts of hawkBit might be infected. **CVE ID : CVE-2019-10240**	053	
kura					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2019	5	In Eclipse Kura versions up to 4.0.0, the SkinServlet did not checked the path passed during servlet call, potentially allowing path traversal in get requests for a limited number of file types. **CVE ID : CVE-2019-10242**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=545835	A-ECL-KURA-010519/76
Information Exposure	09-04-2019	5	In Eclipse Kura versions up to 4.0.0, Kura exposes the underlying Ui Web server version in its replies. This can be used as a hint by an attacker to specifically craft attacks to the web server run by Kura. **CVE ID : CVE-2019-10243**	https://bugs.eclipse.org/bugs/show_bug.cgi?id=545834	A-ECL-KURA-010519/77
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	5	In Eclipse Kura versions up to 4.0.0, the Web UI package and component services, the Artemis simple Mqtt component and the emulator position service (not part of the device distribution) could	https://bugs.eclipse.org/bugs/show_bug.cgi?id=545835	A-ECL-KURA-010519/78

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially be target of XXE attack due to an improper factory and parser initialisation. **CVE ID : CVE-2019-10244**		
Elgg					
elgg					
URL Redirection to Untrusted Site ('Open Redirect')	08-04-2019	5.8	Elgg before 1.12.18 and 2.3.x before 2.3.11 has an open redirect. **CVE ID : CVE-2019-11016**	N/A	A-ELG-ELGG-010519/79
F5					
big-ip_access_policy_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/80
Improper Input	11-04-2019	9	On BIG-IP versions 14.0.0-14.0.0.4, 13.0.0-13.1.1.1,	https://support.f5.com/cs	A-F5-BIG--

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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			12.1.0-12.1.4, 11.6.0-11.6.3.4, and 11.5.1-11.5.8, the system is vulnerable to a denial of service attack when performing URL classification. **CVE ID : CVE-2019-6610**	p/article/K42465020	010519/81
big-ip_advanced_firewall_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/82
big-ip_analytics					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/83

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**		
big-ip_application_acceleration_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/84
big-ip_application_security_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms.	https://support.f5.com/csp/article/K1	A-F5-BIG--010519/85

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	8535734	
big-ip_domain_name_system					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms.	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/86

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-6609		
big-ip_edge_gateway					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/87
big-ip_fraud_protection_service					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/88

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
			as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**		
big-ip_global_traffic_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/89
big-ip_link_controller					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/90

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**		
big-ip_local_traffic_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/91
big-ip_policy_enforcement_manager					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-	https://support.f5.com/csp/article/K1	A-F5-BIG--010519/92

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
			IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	8535734	
big-ip_webaccelerator					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/93

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
big-ip_webaccelerator12.1.1					
N/A	15-04-2019	5	Platform dependent weakness. This issue only impacts iSeries platforms. On these platforms, in BIG-IP APM versions 14.0.0-14.1.0.1, 13.0.0-13.1.1.3, and 12.1.1 HF2-12.1.4, the secureKeyCapable attribute was not set which causes secure vault to not use the F5 hardware support to store the unit key. Instead the unit key is stored in plaintext on disk as would be the case for Z100 systems. Additionally this causes the unit key to be stored in UCS files taken on these platforms. **CVE ID : CVE-2019-6609**	https://support.f5.com/csp/article/K18535734	A-F5-BIG--010519/94
fastadmin					
fastadmin					
Cross-Site Request Forgery (CSRF)	10-04-2019	6	FastAdmin V1.0.0.20190111_beta has a CSRF vulnerability to add a new admin user via the admin/auth/admin/add?dialog=1 URI. **CVE ID : CVE-2019-11077**	N/A	A-FAS-FAST-010519/95
forcepoint					
email_security					
N/A	09-04-2019	7.5	A configuration issue has been discovered in Forcepoint Email Security 8.4.x and 8.5.x: the product	N/A	A-FOR-EMAI-010519/96

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 left in a vulnerable state if the hybrid registration process is not completed. **CVE ID : CVE-2019-6140**		
forticlient					
forticlient					
Improper Access Control	09-04-2019	3.6	An improper access control vulnerability in FortiClientMac before 6.0.5 may allow an attacker to affect the application's performance via modifying the contents of a file used by several FortiClientMac processes. **CVE ID : CVE-2019-5585**	https://fortiguard.com/advisory/FG-IR-19-003	A-FOR-FORT-010519/97
Freedesktop					
poppler					
Out-of-bounds Read	05-04-2019	4.3	An issue was discovered in Poppler 0.74.0. There is a heap-based buffer over-read in the function PSOutputDev::checkPageSlice at PSOutputDev.cc. **CVE ID : CVE-2019-10871**	N/A	A-FRE-POPP-010519/98
Out-of-bounds Read	05-04-2019	6.8	An issue was discovered in Poppler 0.74.0. There is a heap-based buffer over-read in the function Splash::blitTransparent at splash/Splash.cc. **CVE ID : CVE-2019-10872**	N/A	A-FRE-POPP-010519/99
NULL Pointer	05-04-2019	4.3	An issue was discovered in Poppler 0.74.0. There is a NULL pointer dereference	N/A	A-FRE-POPP-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			in the function SplashClip::clipAALine at splash/SplashClip.cc. **CVE ID : CVE-2019-10873**		010519/100
Uncontrolled Resource Consumption	08-04-2019	4.3	FontInfoScanner::scanFonts in FontInfo.cc in Poppler 0.75.0 has infinite recursion, leading to a call to the error function in Error.cc. **CVE ID : CVE-2019-11026**	N/A	A-FRE-POPP-010519/101
gatship					
web_module					
Unrestricted Upload of File with Dangerous Type	09-04-2019	7.5	GAT-Ship Web Module before 1.40 suffers from a vulnerability allowing authenticated attackers to upload any file type to the server via the "Documents" area. This vulnerability is related to "uploadDocFile.aspx". **CVE ID : CVE-2019-11028**	N/A	A-GAT-WEB_-010519/102
Gemalto					
sentinel_ultrapro_client_library					
Uncontrolled Search Path Element	11-04-2019	6.8	The uncontrolled search path element vulnerability in Gemalto Sentinel UltraPro Client Library ux32w.dll Versions 1.3.0, 1.3.1, and 1.3.2 enables an attacker to load and execute a malicious file. **CVE ID : CVE-2019-6534**	https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec131.pdf	A-GEM-SENT-010519/103

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
getbootstrap					
bootstrap-sass					
Improper Control of Generation of Code ('Code Injection')	04-04-2019	10	Arbitrary code execution (via backdoor code) was discovered in bootstrap-sass 3.2.0.3, when downloaded from rubygems.org. An unauthenticated attacker can craft the ___cfduid cookie value with base64 arbitrary code to be executed via eval(), which can be leveraged to execute arbitrary code on the target system. Note that there are three underscore characters in the cookie name. This is unrelated to the __cfduid cookie that is legitimately used by Cloudflare. **CVE ID : CVE-2019-10842**	N/A	A-GET-BOOT-010519/104
gitea					
gitea					
Improper Input Validation	15-04-2019	5	repo/setting.go in Gitea before 1.7.6 and 1.8.x before 1.8-RC3 does not validate the form.MirrorAddress before calling SaveAddress. **CVE ID : CVE-2019-11228**	N/A	A-GIT-GITE-010519/105
Improper Input Validation	15-04-2019	7.5	models/repo_mirror.go in Gitea before 1.7.6 and 1.8.x before 1.8-RC3 mishandles	N/A	A-GIT-GITE-010519/106

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mirror repo URL settings, leading to remote code execution. **CVE ID : CVE-2019-11229**		
Gitlab					
gitlab					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-04-2019	4.3	An issue was discovered in GitLab Community and Enterprise Edition before 11.5.8, 11.6.x before 11.6.6, and 11.7.x before 11.7.1. It allows XSS (issue 2 of 2). **CVE ID : CVE-2019-6796**	N/A	A-GIT-GITL-010519/107
GNU					
gnutls					
Access of Uninitialized Pointer	01-04-2019	5	It was discovered in gnutls before version 3.6.7 upstream that there is an uninitialized pointer access in gnutls versions 3.6.3 or later which can be triggered by certain post-handshake messages. **CVE ID : CVE-2019-3836**	N/A	A-GNU-GNUT-010519/108
gpac					
gpac					
Improper Restriction of Operations within the Bounds of a Memory	15-04-2019	6.8	GPAC 0.7.1 has a buffer overflow issue in gf_import_message() in media_import.c. **CVE ID : CVE-2019-11221**	N/A	A-GPA-GPAC-010519/109

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	15-04-2019	6.8	gf_bin128_parse in utils/os_divers.c in GPAC 0.7.1 has a buffer overflow issue for the crypt feature when encountering a crafted_drm_file.xml file. **CVE ID : CVE-2019-11222**	N/A	A-GPA-GPAC-010519/110
Graphicsmagick					
graphicsmagick					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a stack-based buffer overflow in the function SVGStartElement of coders/svg.c, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a quoted font family value. **CVE ID : CVE-2019-11005**	N/A	A-GRA-GRAP-010519/111
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	6.4	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer over-read in the function ReadMIFFImage of coders/miff.c, which allows attackers to cause a denial of service or information disclosure via an RLE packet. **CVE ID : CVE-2019-11006**	N/A	A-GRA-GRAP-010519/112
Improper	08-04-2019	5.8	In GraphicsMagick 1.4	N/A	A-GRA-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			snapshot-20190322 Q8, there is a heap-based buffer over-read in the ReadMNGImage function of coders/png.c, which allows attackers to cause a denial of service or information disclosure via an image colormap. **CVE ID : CVE-2019-11007**		GRAP-010519/113
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	6.8	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer overflow in the function WriteXWDImage of coders/xwd.c, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file. **CVE ID : CVE-2019-11008**	N/A	A-GRA-GRAP-010519/114
Out-of-bounds Read	08-04-2019	5.8	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a heap-based buffer over-read in the function ReadXWDImage of coders/xwd.c, which allows attackers to cause a denial of service or information disclosure via a crafted image file. **CVE ID : CVE-2019-11009**	N/A	A-GRA-GRAP-010519/115
N/A	08-04-2019	4.3	In GraphicsMagick 1.4 snapshot-20190322 Q8, there is a memory leak in	N/A	A-GRA-GRAP-

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 function ReadMPCImage of coders/mpc.c, which allows attackers to cause a denial of service via a crafted image file. **CVE ID : CVE-2019-11010**		010519/116
Graphviz					
graphviz					
NULL Pointer Dereference	08-04-2019	6.8	The agroot() function in cgraph\obj.c in libcgraph.a in Graphviz 2.39.20160612.1140 has a NULL pointer dereference, as demonstrated by graphml2gv. **CVE ID : CVE-2019-11023**	N/A	A-GRA-GRAP-010519/117
http-live-simulator_project					
http-live-simulator					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	03-04-2019	5	Path traversal vulnerability in http-live-simulator npm package version 1.0.5 allows arbitrary path to be accessed on the file system by a remote attacker. **CVE ID : CVE-2019-5423**	N/A	A-HTT-HTTP-010519/118
IBM					
bigfix_webui_profile_management					
Improper Neutralization of Special Elements used in an SQL	15-04-2019	7.5	IBM BigFix WebUI Profile Management 6 and Software Distribution 23 is vulnerable to SQL injection. A remote attacker could send	N/A	A-IBM-BIGF-010519/119

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			specially-crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 155886. **CVE ID : CVE-2019-4012**		
bigfix_webui_software_distribution					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	15-04-2019	7.5	IBM BigFix WebUI Profile Management 6 and Software Distribution 23 is vulnerable to SQL 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-Force ID: 155886. **CVE ID : CVE-2019-4012**	N/A	A-IBM-BIGF-010519/120
cognos_analytics					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	15-04-2019	6.4	IBM Cognos Analytics 11 could allow a remote attacker to traverse directories on the system. An attacker could send a specially-crafted URL request to write or view arbitrary files on the system. IBM X-Force ID: 158919. **CVE ID : CVE-2019-4178**	N/A	A-IBM-COGN-010519/121
api_connect					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2019	5	Some URIs in IBM API Connect 2018.1 and 2018.4.1.3 disclose system specification information like the machine id, system uuid, filesystem paths, network interface names along with their mac addresses. An attacker can use this information in targeted attacks. IBM X-Force ID: 156542. **CVE ID : CVE-2019-4051**	https://www.ibm.com/support/docview.wss?uid=ibm10879395	A-IBM-API_-010519/122
N/A	08-04-2019	7.5	IBM API Connect's Developer Portal 2018.1 and 2018.4.1.3 is impacted by a privilege escalation vulnerability when integrated with an OpenID Connect (OIDC) user registry. IBM X-Force ID: 158544. **CVE ID : CVE-2019-4155**	N/A	A-IBM-API_-010519/123
Improper Neutralization of Special Elements used in a Command ('Command Injection')	15-04-2019	10	IBM API Connect 5.0.0.0 and 5.0.8.6 Developer Portal is vulnerable to command injection. An attacker with a specially crafted request can run arbitrary code on the server and gain complete access to the system. IBM X-Force ID: 159123. **CVE ID : CVE-2019-4202**	https://www.ibm.com/support/docview.wss?uid=ibm10880109	A-IBM-API_-010519/124
Improper Access	15-04-2019	9	IBM API Connect 5.0.0.0 and 5.0.8.6 Developer Portal can be exploited by	https://www.ibm.com/support/docvi	A-IBM-API_-010519/125

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			app developers to download arbitrary files from the host OS and potentially carry out SSRF attacks. IBM X-Force ID: 159124. **CVE ID : CVE-2019-4203**	ew.wss?uid=ibm10880569	
db2					
Improper Restriction of Operations within the Bounds of a Memory Buffer	03-04-2019	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-Force ID: 155892. **CVE ID : CVE-2019-4014**	https://www.ibm.com/support/docview.wss?uid=ibm10878793	A-IBM-DB2-010519/126
sterling_b2b_integrator					
Improper Restriction of XML External Entity Reference ('XXE')	02-04-2019	5.5	IBM Sterling B2B Integrator Standard Edition 5.2.0 snf 6.0.0.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 156239. **CVE ID : CVE-2019-4043**	https://www.ibm.com/support/docview.wss?uid=ibm10874238	A-IBM-STER-010519/127
websphere_application_server					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	02-04-2019	6.8	IBM WebSphere Application Server Admin Console 7.5, 8.0, 8.5, and 9.0 is vulnerable to a potential denial of service, caused by improper parameter parsing. A remote attacker could exploit this to consume all available CPU resources. IBM X-Force ID: 157380. **CVE ID : CVE-2019-4080**	https://www.ibm.com/support/docview.wss?uid=ibm10875692	A-IBM-WEBS-010519/128
bigfix_platform					
Unrestricted Upload of File with Dangerous Type	10-04-2019	9	IBM BigFix Platform 9.5 could allow any authenticated user to upload any file to any location on the server with root privileges. This results in code execution on underlying system with root privileges. IBM X-Force ID: 155887. **CVE ID : CVE-2019-4013**	N/A	A-IBM-BIGF-010519/129
spectrum_protect					
Improper Access Control	02-04-2019	3.2	IBM Tivoli Storage Manager (IBM Spectrum Protect 8.1.7) could allow a user to restore files and directories using IBM Spectrum Prootect Client Web User Interface on Windows that they should not have access to due to incorrect file permissions. IBM X-Force ID: 157981.	N/A	A-IBM-SPEC-010519/130

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-4093		
qradar_security_information_and_event_manager					
Improper Authentication	08-04-2019	5.5	IBM QRadar SIEM 7.3.2 could allow a user to bypass authentication exposing certain functionality which could lead to information disclosure or modification of application configuration. IBM X-Force ID: 158986. **CVE ID : CVE-2019-4210**	https://www.ibm.com/support/docview.wss?uid=ibm10879913	A-IBM-QRAD-010519/131
business_automation_workflow					
Improper Input Validation	08-04-2019	4	IBM Business Automation Workflow and IBM Business Process Manager 18.0.0.0, 18.0.0.1, and 18.0.0.2 provide embedded document management features. Because of a missing restriction in an API, a client might spoof the last modified by value of a document. IBM X-Force ID: 156241. **CVE ID : CVE-2019-4045**	https://www.ibm.com/support/docview.wss?uid=ibm10870494	A-IBM-BUSI-010519/132
business_process_manager					
Improper Input Validation	08-04-2019	4	IBM Business Automation Workflow and IBM Business Process Manager 18.0.0.0, 18.0.0.1, and 18.0.0.2 provide embedded document management features.	https://www.ibm.com/support/docview.wss?uid=ibm10870494	A-IBM-BUSI-010519/133

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Because of a missing restriction in an API, a client might spoof the last modified by value of a document. IBM X-Force ID: 156241. **CVE ID : CVE-2019-4045**		
cloud_private					
Information Exposure Through Log Files	08-04-2019	2.1	The IBM Cloud Private Key Management Service (IBM Cloud Private 3.1.1 and 3.1.2) could allow a local user to obtain sensitive from the KMS plugin container log. IBM X-Force ID: 158348. **CVE ID : CVE-2019-4143**	https://www.ibm.com/support/docview.wss?uid=ibm10878180	A-IBM-CLOU-010519/134
Imagemagick					
imagemagick					
Out-of-bounds Read	02-04-2019	4.3	LocaleLowercase in MagickCore/locale.c in ImageMagick before 7.0.8-32 allows out-of-bounds access, leading to a SIGSEGV. **CVE ID : CVE-2019-10714**	N/A	A-IMA-IMAG-010519/135
Iobit					
smart_defrag					
Information Exposure	11-04-2019	2.1	SmartDefragDriver.sys (2.0) in IObit Smart Defrag 6 never frees an executable kernel pool that is allocated with user defined bytes and size when IOCTL 0x9C401CC0	N/A	A-IOB-SMAR-010519/136

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
			is called. This kernel pointer can be leaked if the kernel pool becomes a "big" pool. **CVE ID : CVE-2019-6493**		
ivanti					
workspace_control					
N/A	05-04-2019	4.6	An issue was discovered in Ivanti Workspace Control before 10.3.90.0. Local authenticated users with low privileges in a Workspace Control managed session can bypass Workspace Control security features configured for this session by resetting the session context. **CVE ID : CVE-2019-10885**	N/A	A-IVA-WORK-010519/137
Jenkins					
irc					
N/A	04-04-2019	4	Jenkins IRC Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003051**	N/A	A-JEN-IRC-010519/138
aws_elastic_beanstalk_publisher					
N/A	04-04-2019	4	Jenkins AWS Elastic Beanstalk Publisher Plugin stores credentials	N/A	A-JEN-AWS_-010519/139

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003052**		
hockeyapp					
N/A	04-04-2019	4	Jenkins HockeyApp Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003053**	N/A	A-JEN-HOCK-010519/140
jira_issue_updater					
N/A	04-04-2019	4	Jenkins Jira Issue Updater Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003054**	N/A	A-JEN-JIRA-010519/141
ftp_publisher					
N/A	04-04-2019	4	Jenkins FTP publisher Plugin stores credentials unencrypted in its global	N/A	A-JEN-FTP_-010519/142

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003055**		
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins FTP publisher Plugin in the FTPPublisher.DescriptorImpl#doLoginCheck method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003058**	N/A	A-JEN-FTP_-010519/143
N/A	04-04-2019	4	A missing permission check in Jenkins FTP publisher Plugin in the FTPPublisher.DescriptorImpl#doLoginCheck method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003059**	N/A	A-JEN-FTP_-010519/144
websphere_deployer					
N/A	04-04-2019	4	Jenkins WebSphere Deployer Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they	N/A	A-JEN-WEBS-010519/145

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003056**		
bitbucket_approve					
N/A	04-04-2019	4	Jenkins Bitbucket Approve Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003057**	N/A	A-JEN-BITB-010519/146
official_owasp_zap					
N/A	04-04-2019	4	Jenkins Official OWASP ZAP Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003060**	N/A	A-JEN-OFFI-010519/147
jenkins-cloudformation-plugin					
N/A	04-04-2019	4	Jenkins jenkins-cloudformation-plugin Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users	N/A	A-JEN-JENK-010519/148

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003061**		
aws_cloudwatch_logs_publisher					
N/A	04-04-2019	4	Jenkins AWS CloudWatch Logs Publisher Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003062**	N/A	A-JEN-AWS_-010519/149
amazon_sns_build_notifier					
N/A	04-04-2019	4	Jenkins Amazon SNS Build Notifier Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003063**	N/A	A-JEN-AMAZ-010519/150
aws-device-farm					
N/A	04-04-2019	4	Jenkins aws-device-farm Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master	N/A	A-JEN-AWS--010519/151

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			file system. **CVE ID : CVE-2019-1003064**		
cloudshare_docker-machine					
N/A	04-04-2019	4	Jenkins CloudShare Docker-Machine Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003065**	N/A	A-JEN-CLOU-010519/152
bugzilla					
N/A	04-04-2019	4	Jenkins Bugzilla Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003066**	N/A	A-JEN-BUGZ-010519/153
trac_publisher					
N/A	04-04-2019	4	Jenkins Trac Publisher Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to	N/A	A-JEN-TRAC-010519/154

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
			the master file system. **CVE ID : CVE-2019-1003067**		
vmware_vrealize_automation					
N/A	04-04-2019	4	Jenkins VMware vRealize Automation Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003068**	N/A	A-JEN-VMWA-010519/155
aqua_security_scanner					
N/A	04-04-2019	4	Jenkins Aqua Security Scanner Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003069**	N/A	A-JEN-AQUA-010519/156
veracode-scanner					
N/A	04-04-2019	4	Jenkins veracode-scanner Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	N/A	A-JEN-VERA-010519/157

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-1003070		
wildfly_deployer					
N/A	04-04-2019	4	Jenkins WildFly Deployer Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003072**	N/A	A-JEN-WILD-010519/158
vs_team_services_continuous_deployment					
N/A	04-04-2019	4	Jenkins VS Team Services Continuous Deployment Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003073**	N/A	A-JEN-VS_T-010519/159
hyper.sh_commons					
N/A	04-04-2019	4	Jenkins Hyper.sh Commons Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system.	N/A	A-JEN-HYPE-010519/160

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-1003074		
audit_to_database					
N/A	04-04-2019	4	Jenkins Audit to Database Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003075**	N/A	A-JEN-AUDI-010519/161
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Audit to Database Plugin in the DbAuditPublisherDescriptorImpl#doTestJdbcConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003076**	N/A	A-JEN-AUDI-010519/162
N/A	04-04-2019	4	A missing permission check in Jenkins Audit to Database Plugin in the DbAuditPublisherDescriptorImpl#doTestJdbcConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server.	N/A	A-JEN-AUDI-010519/163

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-1003077		
vmware_lab_manager_slaves					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins VMware Lab Manager Slaves Plugin in the LabManager.DescriptorImpl#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003078**	N/A	A-JEN-VMWA-010519/164
N/A	04-04-2019	4	A missing permission check in Jenkins VMware Lab Manager Slaves Plugin in the LabManager.DescriptorImpl#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003079**	N/A	A-JEN-VMWA-010519/165
openshift_deployer					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins OpenShift Deployer Plugin in the DeployApplication.Deploy	N/A	A-JEN-OPEN-010519/166

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ApplicationDescriptor#doCheckLogin form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003080**		
N/A	04-04-2019	4	A missing permission check in Jenkins OpenShift Deployer Plugin in the DeployApplication.DeployApplicationDescriptor#doCheckLogin form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003081**	N/A	A-JEN-OPEN-010519/167
gearman					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Gearman Plugin in the GearmanPluginConfig#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003082**	N/A	A-JEN-GEAR-010519/168
N/A	04-04-2019	4	A missing permission	N/A	A-JEN-GEAR-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			check in Jenkins Gearman Plugin in the GearmanPluginConfig#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003083**		010519/169
zephyr_enterprise_test_management					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Zephyr Enterprise Test Management Plugin in the ZeeDescriptor#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003084**	N/A	A-JEN-ZEPH-010519/170
N/A	04-04-2019	4	A missing permission check in Jenkins Zephyr Enterprise Test Management Plugin in the ZeeDescriptor#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-**	N/A	A-JEN-ZEPH-010519/171

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1003085		
chef_sinatra					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Chef Sinatra Plugin in the ChefBuilderConfiguration.DescriptorImpl#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003086**	N/A	A-JEN-CHEF-010519/172
N/A	04-04-2019	4	A missing permission check in Jenkins Chef Sinatra Plugin in the ChefBuilderConfiguration.DescriptorImpl#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003087**	N/A	A-JEN-CHEF-010519/173
fabric_beta_publisher					
N/A	04-04-2019	4	Jenkins Fabric Beta Publisher Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to	N/A	A-JEN-FABR-010519/174

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the master file system. **CVE ID : CVE-2019-1003088**		
upload_to_pgyer					
N/A	04-04-2019	4	Jenkins Upload to pgyer Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003089**	N/A	A-JEN-UPLO-010519/175
soasta_cloudtest					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins SOASTA CloudTest Plugin in the CloudTestServer.DescriptorImpl#doValidate form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003090**	N/A	A-JEN-SOAS-010519/176
N/A	04-04-2019	4	A missing permission check in Jenkins SOASTA CloudTest Plugin in the CloudTestServer.DescriptorImpl#doValidate form validation method allows attackers with Overall/Read permission	N/A	A-JEN-SOAS-010519/177

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003091**		
nomad					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Nomad Plugin in the NomadCloud.DescriptorImpl#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003092**	N/A	A-JEN-NOMA-010519/178
N/A	04-04-2019	4	A missing permission check in Jenkins Nomad Plugin in the NomadCloud.DescriptorImpl#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003093**	N/A	A-JEN-NOMA-010519/179
open_stf					
N/A	04-04-2019	4	Jenkins Open STF Plugin stores credentials unencrypted in its global configuration file on the	N/A	A-JEN-OPEN-010519/180

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003094**		
perfecto_mobile					
N/A	04-04-2019	4	Jenkins Perfecto Mobile Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003095**	N/A	A-JEN-PERF-010519/181
testfairy					
N/A	04-04-2019	4	Jenkins TestFairy Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-1003096**	N/A	A-JEN-TEST-010519/182
crowd_integration					
N/A	04-04-2019	4	Jenkins Crowd Integration Plugin stores credentials unencrypted in the global config.xml configuration file on the Jenkins master where they can be viewed	N/A	A-JEN-CROW-010519/183

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by users with access to the master file system. **CVE ID : CVE-2019-1003097**		
openid					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003098**	N/A	A-JEN-OPEN-010519/184
N/A	04-04-2019	4	A missing permission check in Jenkins openid Plugin in the OpenIdSsoSecurityRealm.DescriptorImpl#doValidate form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-1003099**	N/A	A-JEN-OPEN-010519/185
starteam					
N/A	04-04-2019	4	Jenkins StarTeam Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they	N/A	A-JEN-STAR-010519/186

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
			can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10277**		
jenkins-reviewbot					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins jenkins-reviewbot Plugin in the ReviewboardDescriptor#doTestConnection form validation method allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-10278**	N/A	A-JEN-JENK-010519/187
N/A	04-04-2019	4	A missing permission check in Jenkins jenkins-reviewbot Plugin in the ReviewboardDescriptor#doTestConnection form validation method allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-10279**	N/A	A-JEN-JENK-010519/188
assembla_auth					
N/A	04-04-2019	4	Jenkins Assembla Auth Plugin stores credentials unencrypted in the global config.xml configuration file on the Jenkins master where they can be viewed	N/A	A-JEN-ASSE-010519/189

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by users with access to the master file system. **CVE ID : CVE-2019-10280**		
relution_enterprise_appstore_publisher					
N/A	04-04-2019	4	Jenkins Relution Enterprise Appstore Publisher Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10281**	N/A	A-JEN-RELU-010519/190
klaros-testmanagement					
N/A	04-04-2019	4	Jenkins Klaros-Testmanagement Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10282**	N/A	A-JEN-KLAR-010519/191
jenkins					
Improper Authenticati on	10-04-2019	6.8	Users who cached their CLI authentication before Jenkins was updated to 2.150.2 and newer, or 2.160 and newer, would remain authenticated in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, because the fix	N/A	A-JEN-JENK-010519/192

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
			for CVE-2019-1003004 in these releases did not reject existing remoting-based CLI authentication caches. **CVE ID : CVE-2019-1003049**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	10-04-2019	3.5	The f:validateButton form control for the Jenkins UI did not properly escape job URLs in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, resulting in a cross-site scripting (XSS) vulnerability exploitable by users with the ability to control job names. **CVE ID : CVE-2019-1003050**	N/A	A-JEN-JENK-010519/193
octopusdeploy					
N/A	04-04-2019	4	Jenkins OctopusDeploy Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-1003071**	N/A	A-JEN-OCTO-010519/194
mabl					
N/A	04-04-2019	4	Jenkins mabl Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they	N/A	A-JEN-MABL-010519/195

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10283**		
diawi_upload					
N/A	04-04-2019	4	Jenkins Diawi Upload Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10284**	N/A	A-JEN-DIAW-010519/196
minio_storage					
N/A	04-04-2019	4	Jenkins Minio Storage Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10285**	N/A	A-JEN-MINI-010519/197
deployhub					
N/A	04-04-2019	4	Jenkins DeployHub Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to	N/A	A-JEN-DEPL-010519/198

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 master file system. **CVE ID : CVE-2019-10286**		
youtrack-plugin					
N/A	04-04-2019	4	Jenkins youtrack-plugin Plugin 0.7.1 and older stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system. **CVE ID : CVE-2019-10287**	N/A	A-JEN-YOUT-010519/199
jabber_server					
N/A	04-04-2019	4	Jenkins Jabber Server Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10288**	N/A	A-JEN-JABB-010519/200
netsparker_cloud_scan					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Netsparker Cloud Scan Plugin 1.1.5 and older in the NCScanBuilder.DescriptorImpl#doValidateAPI form validation method allowed attackers to initiate a connection to an attacker-specified server.	N/A	A-JEN-NETS-010519/201

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-10289		
N/A	04-04-2019	4	A missing permission check in Jenkins Netsparker Cloud Scan Plugin 1.1.5 and older in the NCScanBuilder.DescriptorImpl#doValidateAPI form validation method allowed attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-10290**	N/A	A-JEN-NETS-010519/202
N/A	04-04-2019	4	Jenkins Netsparker Cloud Scan Plugin 1.1.5 and older stored credentials unencrypted in its global configuration file on the Jenkins master where they could be viewed by users with access to the master file system. **CVE ID : CVE-2019-10291**	N/A	A-JEN-NETS-010519/203
kmap					
Cross-Site Request Forgery (CSRF)	04-04-2019	4.3	A cross-site request forgery vulnerability in Jenkins Kmap Plugin in KmapJenkinsBuilder.DescriptorImpl form validation methods allows attackers to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-10292**	N/A	A-JEN-KMAP-010519/204

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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	04-04-2019	4	A missing permission check in Jenkins Kmap Plugin in KmapJenkinsBuilder.DescriptorImpl form validation methods allows attackers with Overall/Read permission to initiate a connection to an attacker-specified server. **CVE ID : CVE-2019-10293**	N/A	A-JEN-KMAP-010519/205
N/A	04-04-2019	4	Jenkins Kmap Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10294**	N/A	A-JEN-KMAP-010519/206
crittercism-dsym					
N/A	04-04-2019	4	Jenkins crittercism-dsym Plugin stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2019-10295**	N/A	A-JEN-CRIT-010519/207
serena_sra_deploy					
N/A	04-04-2019	4	Jenkins Serena SRA Deploy Plugin stores credentials unencrypted in its global	N/A	A-JEN-SERE-010519/208

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10296**		
sametime					
N/A	04-04-2019	4	Jenkins Sametime Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10297**	N/A	A-JEN-SAME-010519/209
koji					
N/A	04-04-2019	4	Jenkins Koji Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10298**	N/A	A-JEN-KOJI-010519/210
cloudcoreo_deploytime					
N/A	04-04-2019	4	Jenkins CloudCoreo DeployTime Plugin stores credentials unencrypted in its global configuration file on the Jenkins master where they can be viewed by users with access to the master file system. **CVE ID : CVE-2019-10299**	N/A	A-JEN-CLOU-010519/211

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Jfrog					
artifactory					
Improper Access Control	11-04-2019	7.5	An issue was discovered in JFrog Artifactory 6.7.3. By default, the access-admin account is used to reset the password of the admin account in case an administrator gets locked out from the Artifactory console. This is only allowable from a connection directly from localhost, but providing a X-Forwarded-For HTTP header to the request allows an unauthenticated user to login with the default credentials of the access-admin account while bypassing the whitelist of allowed IP addresses. The access-admin account can use Artifactory's API to request authentication tokens for all users including the admin account and, in turn, assume full control of all artifacts and repositories managed by Artifactory. **CVE ID : CVE-2019-9733**	https://www.jfrog.com/confluence/display/RTF/Release+Notes#ReleaseNotes-Artifactory6.8.6	A-JFR-ARTI-010519/212
Joomla					
Joomla!					
Improper Limitation of	10-04-2019	7.5	An issue was discovered in Joomla! before 3.9.5. The	N/A	A-JOO-JOOM-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			Media Manager component does not properly sanitize the folder parameter, allowing attackers to act outside the media manager root directory. **CVE ID : CVE-2019-10945**		010519/213
Improper Access Control	10-04-2019	5	An issue was discovered in Joomla! before 3.9.5. The "refresh list of helpsites" endpoint of com_users lacks access checks, allowing calls from unauthenticated users. **CVE ID : CVE-2019-10946**	N/A	A-JOO-JOOM-010519/214
Juniper					
junos					
Improper Input Validation	10-04-2019	5	On Junos devices with the BGP graceful restart helper mode enabled or the BGP graceful restart mechanism enabled, a BGP session restart on a remote peer that has the graceful restart mechanism enabled may cause the local routing protocol daemon (RPD) process to crash and restart. By simulating a specific BGP session restart, an attacker can repeatedly crash the RPD process causing prolonged denial of service (DoS). Graceful restart helper	https://kb.juniper.net/JSA10932	A-JUN-JUNO-010519/215

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mode for BGP is enabled by default. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7; 16.1X65 versions prior to 16.1X65-D48; 16.2 versions prior to 16.2R2-S8; 17.1 versions prior to 17.1R2-S7, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D92, 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R2-S2, 17.3R3; 17.4 versions prior to 17.4R1-S4, 17.4R2; 18.1 versions prior to 18.1R2. Junos OS releases prior to 16.1R1 are not affected. **CVE ID : CVE-2019-0028**		
N/A	10-04-2019	7.2	When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on systems booted from an OAM (Operations, Administration, and	https://kb.juniper.net/JSA10924	A-JUN-JUNO-010519/216

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Maintenance) volume, leading to a possible administrative bypass with physical access to the console. OAM volumes (e.g. flash drives) are typically instantiated as /dev/gpt/oam, or /oam for short. Password recovery, changing the root password from a console, should not have been allowed from an insecure console. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1F6-S12, 15.1R7-S3; 15.1X49 versions prior to 15.1X49-D160; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D496, 15.1X53-D68; 16.1 versions prior to 16.1R3-S10, 16.1R6-S6, 16.1R7-S3; 16.1X65 versions prior to 16.1X65-D49; 16.2 versions prior to 16.2R2-S8; 17.1 versions prior to 17.1R2-S10, 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S3; 17.4 versions prior to 17.4R1-S6, 17.4R2-S2; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to		

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75-D40; 18.3 versions prior to 18.3R1-S2. This issue does not affect Junos OS releases prior to 15.1. **CVE ID : CVE-2019-0035**		
N/A	10-04-2019	7.5	When configuring a stateless firewall filter in Junos OS, terms named using the format "internal-n" (e.g. "internal-1", "internal-2", etc.) are silently ignored. No warning is issued during configuration, and the config is committed without error, but the filter criteria will match all packets leading to unexpected results. Affected releases are Juniper Networks Junos OS: All versions prior to and including 12.3; 14.1X53 versions prior to 14.1X53-D130, 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D161, 15.1X49-D170; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D496, 15.1X53-D69; 16.1 versions prior to 16.1R7-S4, 16.1R7-S5; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2	https://kb.juniper.net/JSA10925	A-JUN-JUNO-010519/217

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S7, 17.4R2-S3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S4; 18.2 versions prior to 18.2R1-S5, 18.2R2-S1; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S3; 18.4 versions prior to 18.4R1-S1, 18.4R1-S2. **CVE ID : CVE-2019-0036**		
k-9_mail_project					
k-9_mail					
N/A	07-04-2019	4.3	K-9 Mail v5.600 can include the original quoted HTML code of a specially crafted, benign looking, email within (digitally signed) reply messages. The quoted part can contain conditional statements that show completely different text if opened in a different email client. This can be abused by an attacker to obtain valid S/MIME or PGP signatures for arbitrary content to be displayed to a third party. NOTE: the vendor states "We don't plan to take any action because of this."	N/A	A-K-9-K-9_-010519/218

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-10741		
kakaocorp					
kakaotalk					
Improper Input Validation	01-04-2019	6.8	Remote code execution vulnerability exists in KaKaoTalk PC messenger when user clicks specially crafted link in the message window. This affects KaKaoTalk windows version 2.7.5.2024 or lower. **CVE ID : CVE-2019-9132**	https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=34981	A-KAK-KAKA-010519/219
KDE					
kmail					
N/A	07-04-2019	4.3	In KDE KMail 5.2.3, an attacker in possession of S/MIME or PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, they unknowingly leak the plaintext of the encrypted message part(s) back to the attacker. **CVE ID : CVE-2019-10732**	N/A	A-KDE-KMAI-010519/220

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kmplayer					
kmplayer					
Integer Underflow (Wrap or Wraparound)	09-04-2019	4.3	When processing subtitles format media file, KMPlayer version 2018.12.24.14 or lower doesn't check object size correctly, which leads to integer underflow then to memory out-of-bound read/write. An attacker can exploit this issue by enticing an unsuspecting user to open a malicious file. **CVE ID : CVE-2019-9133**	N/A	A-KMP-KMPL-010519/221
Kubernetes					
kubernetes					
Uncontrolled Resource Consumption	01-04-2019	4	In all Kubernetes versions prior to v1.11.8, v1.12.6, and v1.13.4, users that are authorized to make patch requests to the Kubernetes API Server can send a specially crafted patch of type "json-patch" (e.g. `kubectl patch --type json` or `"Content-Type: application/json-patch+json"`) that consumes excessive resources while processing, causing a Denial of Service on the API Server. **CVE ID : CVE-2019-**	https://security.netapp.com/advisory/ntap-20190416-0002/	A-KUB-KUBE-010519/222

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			1002100		
Improper Link Resolution Before File Access ('Link Following')	01-04-2019	5.8	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes creates a tar inside the container, copies it over the network, and kubectl unpacks it on the user?s machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user?s machine when kubectl cp is called, limited only by the system permissions of the local user. The untar function can both create and follow symbolic links. The issue is resolved in kubectl v1.11.9, v1.12.7, v1.13.5, and v1.14.0. **CVE ID : CVE-2019-1002101**	N/A	A-KUB-KUBE-010519/223
N/A	02-04-2019	5	Cloud Native Computing Foundation (CNCF) CNI (Container Networking Interface) 0.7.4 has a network firewall misconfiguration which affects Kubernetes. The CNI 'portmap' plugin, used to setup HostPorts for CNI,	https://security.netapp.com/advisory/ntap-20190416-0002/	A-KUB-KUBE-010519/224

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inserts rules at the front of the iptables nat chains; which take precedence over the KUBE- SERVICES chain. Because of this, the HostPort/portmap rule could match incoming traffic even if there were better fitting, more specific service definition rules like NodePorts later in the chain. The issue is fixed in CNI 0.7.5 and Kubernetes 1.11.9, 1.12.7, 1.13.5, and 1.14.0. **CVE ID : CVE-2019-9946**		
libsixel_project					
libsixel					
Improper Input Validation	08-04-2019	4.3	The load_pnm function in frompnm.c in libsixel.a in libsixel 1.8.2 has infinite recursion. **CVE ID : CVE-2019-11024**	N/A	A-LIB-LIBS-010519/225
Lighttpd					
lighttpd					
Integer Overflow or Wraparound	10-04-2019	7.5	** DISPUTED ** lighttpd before 1.4.54 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a malicious HTTP GET request, as demonstrated by mishandling of /%2F?	N/A	A-LIG-LIGH-010519/226

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in burl_normalize_2F_to_slash_fix in burl.c. NOTE: The developer states "The feature which can be abused to cause the crash is a new feature in lighttpd 1.4.50, and is not enabled by default. It must be explicitly configured in the config file (e.g. lighttpd.conf). Certain input will trigger an abort() in lighttpd when that feature is enabled. lighttpd detects the underflow or realloc() will fail (in both 32-bit and 64-bit executables), also detected in lighttpd. Either triggers an explicit abort() by lighttpd. This is not exploitable beyond triggering the explicit abort() with subsequent application exit." **CVE ID : CVE-2019-11072**		
Magento					
magento					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	10-04-2019	7.5	An unauthenticated user can execute arbitrary code through an SQL injection vulnerability, which causes sensitive data leakage. This issue is fixed in Magento Open Source 1.9.4.1, Magento	N/A	A-MAG-MAGE-010519/227

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			Commerce 1.14.4.1, SUPEE-11086, Magento 2.2.8, Magento 2.3.1. **CVE ID : CVE-2019-7139**		
materializecss					
materialize					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	4.3	In Materialize through 1.0.0, XSS is possible via the Tooltip feature. **CVE ID : CVE-2019-11002**	N/A	A-MAT-MATE-010519/228
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	4.3	In Materialize through 1.0.0, XSS is possible via the Autocomplete feature. **CVE ID : CVE-2019-11003**	N/A	A-MAT-MATE-010519/229
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	4.3	In Materialize through 1.0.0, XSS is possible via the Toast feature. **CVE ID : CVE-2019-11004**	N/A	A-MAT-MATE-010519/230
Matrixssl					
matrixssl					
Improper Restriction of Operations	08-04-2019	7.5	pubRsaDecryptSignedElementExt in MatrixSSL, as used in Inside Secure TLS Toolkit, through 4.0.2	N/A	A-MAT-MATR-010519/231

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Open has a stack-based buffer overflow during X.509 certificate verification because of missing validation in psRsaDecryptPubExt in crypto/pubkey/rsa_pub.c. **CVE ID : CVE-2019-10914**		
mi					
mi_browser					
Improper Input Validation	05-04-2019	4.3	A URL spoofing vulnerability was found in all international versions of Xiaomi Mi browser 10.5.6-g (aka the MIUI native browser) and Mint Browser 1.5.3 due to the way they handle the "q" query parameter. The portion of an https URL before the ?q= substring is not shown to the user. **CVE ID : CVE-2019-10875**	N/A	A-MI-MI_B-010519/232
mint_browser					
Improper Input Validation	05-04-2019	4.3	A URL spoofing vulnerability was found in all international versions of Xiaomi Mi browser 10.5.6-g (aka the MIUI native browser) and Mint Browser 1.5.3 due to the way they handle the "q" query parameter. The portion of an https URL before the ?q= substring is not shown to the user.	N/A	A-MI-MINT-010519/233

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-10875		
Microfocus					
content_manager					
Unrestricted Upload of File with Dangerous Type	01-04-2019	5	An unauthenticated file upload vulnerability has been identified in the Web Client component of Micro Focus Content Manager 9.1, 9.2, and 9.3 when configured to use the ADFS authentication method. The vulnerability could be exploited by an unauthenticated remote attacker to upload content to arbitrary locations on the Content Manager server. **CVE ID : CVE-2019-3489**	N/A	A-MIC-CONT-010519/234
Microsoft					
.net_core_sdk					
Improper Access Control	08-04-2019	4	A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify a NuGet package's folder structure, aka 'NuGet Package Manager Tampering Vulnerability'. **CVE ID : CVE-2019-0757**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0757	A-MIC-.NET-010519/235
nuget					
Improper Access	08-04-2019	4	A tampering vulnerability exists in the NuGet	https://portal.msrc.micr	A-MIC-NUGE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Control			Package Manager for Linux and Mac that could allow an authenticated attacker to modify a NuGet package's folder structure, aka 'NuGet Package Manager Tampering Vulnerability'. **CVE ID : CVE-2019-0757**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0757	010519/236
lync_server					
Improper Input Validation	08-04-2019	4.3	A spoofing vulnerability exists when a Lync Server or Skype for Business Server does not properly sanitize a specially crafted request, aka 'Skype for Business and Lync Spoofing Vulnerability'. **CVE ID : CVE-2019-0798**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0798	A-MIC-LYNC-010519/237
skype_for_business_server					
Improper Input Validation	08-04-2019	4.3	A spoofing vulnerability exists when a Lync Server or Skype for Business Server does not properly sanitize a specially crafted request, aka 'Skype for Business and Lync Spoofing Vulnerability'. **CVE ID : CVE-2019-0798**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0798	A-MIC-SKYP-010519/238
chakracore					
Improper Restriction of Operations within the Bounds of a	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-CHAK-010519/239

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Buffer			'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0611. **CVE ID : CVE-2019-0592**	2019-0592	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0609**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609	A-MIC-CHAK-010519/240
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0592. **CVE ID : CVE-2019-0611**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0611	A-MIC-CHAK-010519/241
Improper Restriction of Operations	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in	N/A	A-MIC-CHAK-010519/242

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0752, CVE-2019-0753, CVE-2019-0862. **CVE ID : CVE-2019-0739**		
Information Exposure	08-04-2019	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'. **CVE ID : CVE-2019-0746**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0746	A-MIC-CHAK-010519/243
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0769	A-MIC-CHAK-010519/244
Improper Restriction of Operations	08-04-2019	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-010519/245

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0771**	guidance/advisory/CVE-2019-0771	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0783. **CVE ID : CVE-2019-0773**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0773	A-MIC-CHAK-010519/246
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810,	N/A	A-MIC-CHAK-010519/247

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0812, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0829**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0806**	N/A	A-MIC-CHAK-010519/248
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0810**	N/A	A-MIC-CHAK-010519/249
Improper Restriction of	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra	N/A	A-MIC-CHAK-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0812**		010519/250
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0861. **CVE ID : CVE-2019-0860**	N/A	A-MIC-CHAK-010519/251
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	A-MIC-CHAK-010519/252

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860. **CVE ID : CVE-2019-0861**		
edge					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0611. **CVE ID : CVE-2019-0592**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0592	A-MIC-EDGE-010519/253
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0609**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609	A-MIC-EDGE-010519/254
Improper Restriction of	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra	https://portal.msrc.microsoft.com/en	A-MIC-EDGE-010519/255

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0592. **CVE ID : CVE-2019-0611**	-US/security-guidance/advisory/CVE-2019-0611	
N/A	08-04-2019	2.6	A security feature bypass vulnerability exists when Click2Play protection in Microsoft Edge improperly handles flash objects. By itself, this bypass vulnerability does not allow arbitrary code execution, aka 'Microsoft Edge Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0612**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0612	A-MIC-EDGE-010519/256
N/A	08-04-2019	4	An elevation of privilege vulnerability exists when Microsoft Edge does not properly enforce cross-domain policies, which could allow an attacker to access information from one domain and inject it into another domain.In a web-based attack scenario, an attacker could host a website that is used to attempt to exploit the vulnerability, aka 'Microsoft Edge Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0678	A-MIC-EDGE-010519/257

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0678		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0752, CVE-2019-0753, CVE-2019-0862. **CVE ID : CVE-2019-0739**	N/A	A-MIC-EDGE-010519/258
Information Exposure	08-04-2019	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'. **CVE ID : CVE-2019-0746**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0746	A-MIC-EDGE-010519/259
N/A	08-04-2019	4.3	A security feature bypass vulnerability exists when Microsoft browsers improperly handle requests of different origins, aka 'Microsoft Browsers Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0762	A-MIC-EDGE-010519/260
Improper Input Validation	09-04-2019	4.3	A tampering vulnerability exists when Microsoft browsers do not properly validate input under	N/A	A-MIC-EDGE-010519/261

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific conditions, aka 'Microsoft Browsers Tampering Vulnerability'. **CVE ID : CVE-2019-0764**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0769**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0769	A-MIC-EDGE-010519/262
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0770**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0770	A-MIC-EDGE-010519/263
Improper Restriction of	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting	https://portal.msrc.microsoft.com/en	A-MIC-EDGE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			engine handles objects in memory in Microsoft Edge, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0771**	-US/security-guidance/advisory/CVE-2019-0771	010519/264
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0783. **CVE ID : CVE-2019-0773**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0773	A-MIC-EDGE-010519/265
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists when Microsoft Edge improperly accesses objects in memory, aka 'Microsoft Edge Memory Corruption Vulnerability'. **CVE ID : CVE-2019-0779**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0779	A-MIC-EDGE-010519/266
Improper Restriction	08-04-2019	7.6	A remote code execution vulnerability exists in the	https://portal.msrc.micr	A-MIC-EDGE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2019-0780**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0780	010519/267
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0829**	N/A	A-MIC-EDGE-010519/268
Information Exposure	09-04-2019	4.3	An information disclosure vulnerability exists when Microsoft Edge improperly handles objects in memory, aka 'Microsoft Edge Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0833**	N/A	A-MIC-EDGE-010519/269
Improper Restriction of Operations within the Bounds of a Memory	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption	N/A	A-MIC-EDGE-010519/270

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Vulnerability'. This CVE ID is unique from CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0806**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0810**	N/A	A-MIC-EDGE-010519/271
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0829, CVE-2019-0860, CVE-2019-0861. **CVE ID : CVE-2019-0812**	N/A	A-MIC-EDGE-010519/272

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0861. **CVE ID : CVE-2019-0860**	N/A	A-MIC-EDGE-010519/273
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the Chakra scripting engine handles objects in memory in Microsoft Edge, aka 'Chakra Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0806, CVE-2019-0810, CVE-2019-0812, CVE-2019-0829, CVE-2019-0860. **CVE ID : CVE-2019-0861**	N/A	A-MIC-EDGE-010519/274
office					
Improper Restriction of Operations within the Bounds of a	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-OFFI-010519/275

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Buffer			'Microsoft Office Access Connectivity Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0748**	2019-0748	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that Microsoft Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0822**	N/A	A-MIC-OFFI-010519/276
Improper Input Validation	09-04-2019	6.8	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-2019-0824, CVE-2019-0825, CVE-2019-0826, CVE-2019-0827. **CVE ID : CVE-2019-0823**	N/A	A-MIC-OFFI-010519/277
Improper Input Validation	09-04-2019	6.8	A remote code execution vulnerability exists when the Microsoft Office Access Connectivity Engine improperly handles objects in memory, aka 'Microsoft Office Access Connectivity Engine	N/A	A-MIC-OFFI-010519/278

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0823, CVE-2019-0825, CVE-2019-0826, CVE-2019-0827. **CVE ID : CVE-2019-0824**		
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0826, CVE-2019-0827. **CVE ID : CVE-2019-0825**	N/A	A-MIC-OFFI-010519/279
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0825, CVE-2019-0827. **CVE ID : CVE-2019-0826**	N/A	A-MIC-OFFI-010519/280

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0825, CVE-2019-0826. **CVE ID : CVE-2019-0827**	N/A	A-MIC-OFFI-010519/281
N/A	09-04-2019	6.8	A remote code execution vulnerability exists when Microsoft Office fails to properly handle certain files.To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file that points to an Excel or PowerPoint file that was also downloaded.The update addresses the vulnerability by correcting how Office handles these files., aka 'Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0801**	N/A	A-MIC-OFFI-010519/282
office_365_proplus					
Improper Restriction of	09-04-2019	9.3	A remote code execution vulnerability exists in the way that Microsoft	N/A	A-MIC-OFFI-010519/283

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Graphics Components handle objects in memory, aka 'Microsoft Graphics Components Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0822**		
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0825, CVE-2019-0826, CVE-2019-0827. **CVE ID : CVE-2019-0824**	N/A	A-MIC-OFFI-010519/284
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0826, CVE-2019-0827. **CVE ID : CVE-2019-0825**	N/A	A-MIC-OFFI-010519/285

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
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0825, CVE-2019-0827. **CVE ID : CVE-2019-0826**	N/A	A-MIC-OFFI-010519/286
Improper Input Validation	09-04-2019	6.8	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-2019-0823, CVE-2019-0824, CVE-2019-0825, CVE-2019-0826. **CVE ID : CVE-2019-0827**	N/A	A-MIC-OFFI-010519/287
Improper Restriction of Operations within the Bounds of a Memory	09-04-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code	N/A	A-MIC-OFFI-010519/288

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Execution Vulnerability'. **CVE ID : CVE-2019-0828**		
N/A	09-04-2019	6.8	A remote code execution vulnerability exists when Microsoft Office fails to properly handle certain files.To exploit the vulnerability, an attacker would have to convince a user to open a specially crafted URL file that points to an Excel or PowerPoint file that was also downloaded.The update addresses the vulnerability by correcting how Office handles these files., aka 'Office Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0801**	N/A	A-MIC-OFFI-010519/289
internet_explorer					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way the scripting engine handles objects in memory in Microsoft browsers, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0609**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609	A-MIC-INTE-010519/290

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ChakraCore scripting engine handles objects in memory, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0639**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0639	A-MIC-INTE-010519/291
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0666, CVE-2019-0667, CVE-2019-0772. **CVE ID : CVE-2019-0665**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0665	A-MIC-INTE-010519/292
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0667,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0666	A-MIC-INTE-010519/293

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE-2019-0772. **CVE ID : CVE-2019-0666**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0772. **CVE ID : CVE-2019-0667**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0667	A-MIC-INTE-010519/294
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773, CVE-2019-0783. **CVE ID : CVE-2019-0680**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0680	A-MIC-INTE-010519/295
Information Exposure	08-04-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory in Microsoft Edge, aka 'Scripting Engine	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-INTE-010519/296

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0746**	2019-0746	
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0739, CVE-2019-0753, CVE-2019-0862. **CVE ID : CVE-2019-0752**	N/A	A-MIC-INTE-010519/297
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0739, CVE-2019-0752, CVE-2019-0862. **CVE ID : CVE-2019-0753**	N/A	A-MIC-INTE-010519/298
N/A	08-04-2019	4.3	A security feature bypass vulnerability exists when Internet Explorer fails to validate the correct Security Zone of requests for specific URLs, aka 'Internet Explorer Security Feature Bypass	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0761	A-MIC-INTE-010519/299

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0768. **CVE ID : CVE-2019-0761**		
N/A	08-04-2019	4.3	A security feature bypass vulnerability exists when Microsoft browsers improperly handle requests of different origins, aka 'Microsoft Browsers Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0762**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0762	A-MIC-INTE-010519/300
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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-2019-0763**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0763	A-MIC-INTE-010519/301
Improper Input Validation	09-04-2019	4.3	A tampering vulnerability exists when Microsoft browsers do not properly validate input under specific conditions, aka 'Microsoft Browsers Tampering Vulnerability'. **CVE ID : CVE-2019-0764**	N/A	A-MIC-INTE-010519/302
N/A	08-04-2019	4.3	A security feature bypass vulnerability exists when Internet Explorer VBScript execution policy does not properly restrict VBScript under specific conditions, and to allow requests that	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0768	A-MIC-INTE-010519/303

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			should otherwise be ignored, aka 'Internet Explorer Security Feature Bypass Vulnerability'. This CVE ID is unique from CVE-2019-0761. **CVE ID : CVE-2019-0768**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that Microsoft browsers access objects in memory, aka 'Microsoft Browser Memory Corruption Vulnerability'. **CVE ID : CVE-2019-0780**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0780	A-MIC-INTE-010519/304
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0609, CVE-2019-0639, CVE-2019-0680, CVE-2019-0769, CVE-2019-0770, CVE-2019-0771, CVE-2019-0773. **CVE ID : CVE-2019-0783**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0783	A-MIC-INTE-010519/305
Information Exposure	09-04-2019	4.3	An information disclosure vulnerability exists when the scripting engine does not properly handle objects in memory, aka 'Microsoft Scripting Engine	N/A	A-MIC-INTE-010519/306

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0835**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.6	A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer, aka 'Scripting Engine Memory Corruption Vulnerability'. This CVE ID is unique from CVE-2019-0739, CVE-2019-0752, CVE-2019-0753. **CVE ID : CVE-2019-0862**	N/A	A-MIC-INTE-010519/307
visual_studio_2017					
Improper Access Control	08-04-2019	4	A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify a NuGet package's folder structure, aka 'NuGet Package Manager Tampering Vulnerability'. **CVE ID : CVE-2019-0757**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0757	A-MIC-VISU-010519/308
Untrusted Search Path	08-04-2019	6.8	A remote code execution vulnerability exists when the Visual Studio C++ Redistributable Installer improperly validates input before loading dynamic link library (DLL) files, aka 'Visual Studio Remote	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0809	A-MIC-VISU-010519/309

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Code Execution Vulnerability'. **CVE ID : CVE-2019-0809**		
asp.net_core					
N/A	09-04-2019	5	A denial of service vulnerability exists when ASP.NET Core improperly handles web requests, aka 'ASP.NET Core Denial of Service Vulnerability'. **CVE ID : CVE-2019-0815**	N/A	A-MIC-ASP.-010519/310
sharepoint_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-0831. **CVE ID : CVE-2019-0830**	N/A	A-MIC-SHAR-010519/311
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS	N/A	A-MIC-SHAR-010519/312

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vulnerability'. This CVE ID is unique from CVE-2019-0830. **CVE ID : CVE-2019-0831**		
sharepoint_enterprise_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. **CVE ID : CVE-2019-0778**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0778	A-MIC-SHAR-010519/313
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-0831. **CVE ID : CVE-2019-0830**	N/A	A-MIC-SHAR-010519/314
Improper Neutralization of Input During Web Page	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a	N/A	A-MIC-SHAR-010519/315

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-0830. **CVE ID : CVE-2019-0831**		
exchange_server					
N/A	09-04-2019	5.8	A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests, aka 'Microsoft Exchange Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0858. **CVE ID : CVE-2019-0817**	N/A	A-MIC-EXCH-010519/316
Improper Input Validation	09-04-2019	4.3	A spoofing vulnerability exists in Microsoft Exchange Server when Outlook Web Access (OWA) fails to properly handle web requests, aka 'Microsoft Exchange Spoofing Vulnerability'. This CVE ID is unique from CVE-2019-0817. **CVE ID : CVE-2019-0858**	N/A	A-MIC-EXCH-010519/317
sharepoint_foundation					
Improper Neutralization of Input	08-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft	https://portal.msrc.microsoft.com/en	A-MIC-SHAR-010519/318

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. **CVE ID : CVE-2019-0778**	-US/security-guidance/advisory/CVE-2019-0778	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-0831. **CVE ID : CVE-2019-0830**	N/A	A-MIC-SHAR-010519/319
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	A cross-site-scripting (XSS) vulnerability exists when Microsoft SharePoint Server does not properly sanitize a specially crafted web request to an affected SharePoint server, aka 'Microsoft Office SharePoint XSS Vulnerability'. This CVE ID is unique from CVE-2019-0830. **CVE ID : CVE-2019-0831**	N/A	A-MIC-SHAR-010519/320

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
team_foundation_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-04-2019	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'. **CVE ID : CVE-2019-0777**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0777	A-MIC-TEAM-010519/321
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0867, CVE-2019-0868, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0866**	N/A	A-MIC-TEAM-010519/322
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting	N/A	A-MIC-TEAM-010519/323

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0866, CVE-2019-0868, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0867**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0866, CVE-2019-0867, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0868**	N/A	A-MIC-TEAM-010519/324
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0866, CVE-2019-0867, CVE-2019-0868, CVE-2019-0871.	N/A	A-MIC-TEAM-010519/325

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-0870		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0866, CVE-2019-0867, CVE-2019-0868, CVE-2019-0870. **CVE ID : CVE-2019-0871**	N/A	A-MIC-TEAM-010519/326
excel					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in Microsoft Excel software when the software fails to properly handle objects in memory, aka 'Microsoft Excel Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0828**	N/A	A-MIC-EXCE-010519/327
open_enclave_software_development_kit					
Information Exposure	09-04-2019	4.3	An information disclosure vulnerability exists when affected Open Enclave SDK versions improperly handle objects in memory, aka 'Open Enclave SDK Information Disclosure Vulnerability'.	N/A	A-MIC-OPEN-010519/328

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0876		
mkcms_project					
mkcms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2019	7.5	MKCMS V5.0 has SQL injection via the bplay.php play parameter. **CVE ID : CVE-2019-10707**	N/A	A-MKC-MKCM-010519/329
Cross-Site Request Forgery (CSRF)	10-04-2019	6.8	MKCMS V5.0 has a CSRF vulnerability to add a new admin user via the ucenter/userinfo.php URI. **CVE ID : CVE-2019-11078**	N/A	A-MKC-MKCM-010519/330
Mono-project					
mono_framework					
Improper Access Control	08-04-2019	4	A tampering vulnerability exists in the NuGet Package Manager for Linux and Mac that could allow an authenticated attacker to modify a NuGet package's folder structure, aka 'NuGet Package Manager Tampering Vulnerability'. **CVE ID : CVE-2019-0757**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0757	A-MON-MONO-010519/331
Netapp					
cloud_insights					
N/A	02-04-2019	5	Cloud Native Computing Foundation (CNCF) CNI (Container Networking	https://security.netapp.com/advisory	A-NET-CLOU-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Interface) 0.7.4 has a network firewall misconfiguration which affects Kubernetes. The CNI 'portmap' plugin, used to setup HostPorts for CNI, inserts rules at the front of the iptables nat chains; which take precedence over the KUBE- SERVICES chain. Because of this, the HostPort/portmap rule could match incoming traffic even if there were better fitting, more specific service definition rules like NodePorts later in the chain. The issue is fixed in CNI 0.7.5 and Kubernetes 1.11.9, 1.12.7, 1.13.5, and 1.14.0. **CVE ID : CVE-2019-9946**	/ntap-20190416-0002/	010519/332
Omron					
common_components					
Use After Free	10-04-2019	6.8	When processing project files, the application (Omron CX-Programmer v9.70 and prior and Common Components January 2019 and prior) fails to check if it is referencing freed memory. An attacker could use a specially crafted project file to exploit and execute code under the privileges of the application.	N/A	A-OMR-COMM-010519/333

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-6556		
cx-programmer					
Use After Free	10-04-2019	6.8	When processing project files, the application (Omron CX-Programmer v9.70 and prior and Common Components January 2019 and prior) fails to check if it is referencing freed memory. An attacker could use a specially crafted project file to exploit and execute code under the privileges of the application. **CVE ID : CVE-2019-6556**	N/A	A-OMR-CX-P-010519/334
Openstack					
neutron					
N/A	05-04-2019	4	An issue was discovered in OpenStack Neutron 11.x before 11.0.7, 12.x before 12.0.6, and 13.x before 13.0.3. By creating two security groups with separate/overlapping port ranges, an authenticated user may prevent Neutron from being able to configure networks on any compute nodes where those security groups are present, because of an Open vSwitch (OVS) firewall KeyError. All Neutron deployments utilizing neutron-openvswitch-agent are	https://security.openstack.org/ossa/OSSA-2019-002.html	A-OPE-NEUT-010519/335

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected. **CVE ID : CVE-2019-10876**		
overit					
geocall					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-04-2019	4.3	Multiple XSS vulnerabilities were discovered in OverIT Geocall 6.3 before build 2:346977. **CVE ID : CVE-2019-5888**	N/A	A-OVE-GEOC-010519/336
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-04-2019	5	An log-management directory traversal issue was discovered in OverIT Geocall 6.3 before build 2:346977. **CVE ID : CVE-2019-5889**	N/A	A-OVE-GEOC-010519/337
Improper Authentication	01-04-2019	9	An issue was discovered in OverIT Geocall 6.3 before build 2:346977. Weak authentication and session management allows an authenticated user to obtain access to the Administrative control panel and execute administrative functions. **CVE ID : CVE-2019-5890**	N/A	A-OVE-GEOC-010519/338
Improper Access Control	01-04-2019	5	An issue was discovered in OverIT Geocall 6.3 before build 2:346977. An unauthenticated servlet allows an attacker to	N/A	A-OVE-GEOC-010519/339

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			obtain a cookie of an authenticated user, and login to the web application. **CVE ID : CVE-2019-5891**		
Paloaltonetworks					
expedition_migration_tool					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	The Expedition Migration tool 1.1.6 and earlier may allow an authenticated attacker to run arbitrary JavaScript or HTML in the User Mapping Settings. **CVE ID : CVE-2019-1567**	N/A	A-PAL-EXPE-010519/340
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-04-2019	3.5	Cross-site scripting (XSS) vulnerability in Palo Alto Networks Expedition Migration tool 1.1.12 and earlier may allow an authenticated attacker to run arbitrary JavaScript or HTML in the Devices View. **CVE ID : CVE-2019-1574**	https://securityadvisories.paloaltonetworks.com/Home/Detail/147	A-PAL-EXPE-010519/341
globalprotect					
Improper Authentication	09-04-2019	7.5	GlobalProtect Agent 4.1.0 for Windows and GlobalProtect Agent 4.1.10 and earlier for macOS may allow an attacker to access authentication and/or session tokens and replay them to spoof the VPN session and gain access as the user.	N/A	A-PAL-GLOB-010519/342

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
			CVE ID : CVE-2019-1573		
Pimcore					
pimcore					
Improper Control of Generation of Code ('Code Injection')	04-04-2019	6.5	An issue was discovered in Pimcore before 5.7.1. An attacker with classes permission can send a POST request to /admin/class/bulk-commit, which will make it possible to exploit the unserialize function when passing untrusted values in the data parameter to bundles/AdminBundle/Controller/Admin/DataObject/ClassController.php. **CVE ID : CVE-2019-10867**	N/A	A-PIM-PIMC-010519/343
pivotal_software					
concourse					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-04-2019	5	Pivotal Concourse version 5.0.0, contains an API that is vulnerable to SQL injection. An Concourse resource can craft a version identifier that can carry a SQL injection payload to the Concourse server, allowing the attacker to read privileged data. **CVE ID : CVE-2019-3792**	https://pivotal.io/security/cve-2019-3792	A-PIV-CONC-010519/344
spring_security					
Insufficient Entropy in	09-04-2019	5	Spring Security versions 4.2.x prior to 4.2.12, 5.0.x	https://pivotal.io/security	A-PIV-SPRI-010519/345

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
PRNG			prior to 5.0.12, and 5.1.x prior to 5.1.5 contain an insecure randomness vulnerability when using SecureRandomFactoryBean#setSeed to configure a SecureRandom instance. In order to be impacted, an honest application must provide a seed and make the resulting random material available to an attacker for inspection. **CVE ID : CVE-2019-3795**	/cve-2019-3795	
Plataformatec					
devise					
N/A	03-04-2019	7.5	Plataformatec Devise version 4.5.0 and earlier, using the lockable module contains a CWE-367 vulnerability in The `Devise::Models::Lockable` class, more specifically at the `#increment_failed_attempts` method. File location: lib/devise/models/lockable.rb that can result in Multiple concurrent requests can prevent an attacker from being blocked on brute force attacks. This attack appear to be exploitable via Network connectivity - brute force attacks. This vulnerability appears to	N/A	A-PLA-DEVI-010519/346

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have been fixed in 4.6.0 and later. **CVE ID : CVE-2019-5421**		
podofo_project					
podofo					
N/A	03-04-2019	4.3	An issue was discovered in PoDoFo 0.9.6. The PdfPagesTreeCache class in doc/PdfPagesTreeCache.cpp has an attempted excessive memory allocation because nInitialSize is not validated. **CVE ID : CVE-2019-10723**	N/A	A-POD-PODO-010519/347
Postgresql					
postgresql					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	01-04-2019	9	** DISPUTED ** In PostgreSQL 9.3 through 11.2, the "COPY TO/FROM PROGRAM" function allows superusers and users in the 'pg_read_server_files' group to execute arbitrary code in the context of the database's operating system user. This functionality is enabled by default and can be abused to run arbitrary operating system commands on Windows, Linux, and macOS. NOTE: Third parties claim/state this is	N/A	A-POS-POST-010519/348

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not an issue because PostgreSQL functionality for ?COPY TO/FROM PROGRAM? is acting as intended. References state that in PostgreSQL, a superuser can execute commands as the server user without using the ?COPY FROM PROGRAM?. Furthermore, members in 'pg_read_server_files' can run commands only if either the 'pg_execute_server_program' role or superuser are granted. **CVE ID : CVE-2019-9193**		
Pulsesecure					
pulse_connect_secure					
Session Fixation	12-04-2019	6.8	In Pulse Secure Pulse Desktop Client and Network Connect, an attacker could access session tokens to replay and spoof sessions, and as a result, gain unauthorized access as an end user, a related issue to CVE-2019-1573. (The endpoint would need to be already compromised for exploitation to succeed.) This affects Pulse Desktop Client 5.x before Secure Desktop 5.3R7 and Pulse Desktop Client 9.x before	N/A	A-PUL-PULS-010519/349

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Secure Desktop 9.0R3. It also affects (for Network Connect customers) Pulse Connect Secure 8.1 before 8.1R14, 8.3 before 8.3R7, and 9.0 before 9.0R3. **CVE ID : CVE-2019-11213**		
pulse_secure_desktop_client					
Session Fixation	12-04-2019	6.8	In Pulse Secure Pulse Desktop Client and Network Connect, an attacker could access session tokens to replay and spoof sessions, and as a result, gain unauthorized access as an end user, a related issue to CVE-2019-1573. (The endpoint would need to be already compromised for exploitation to succeed.) This affects Pulse Desktop Client 5.x before Secure Desktop 5.3R7 and Pulse Desktop Client 9.x before Secure Desktop 9.0R3. It also affects (for Network Connect customers) Pulse Connect Secure 8.1 before 8.1R14, 8.3 before 8.3R7, and 9.0 before 9.0R3. **CVE ID : CVE-2019-11213**	N/A	A-PUL-PULS-010519/350
Python					
urllib3					
Improper Neutralizatio	15-04-2019	4.3	In the urllib3 library through 1.24.1 for Python,	N/A	A-PYT-URLL-

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 of CRLF Sequences ('CRLF Injection')			CRLF injection is possible if the attacker controls the request parameter. **CVE ID : CVE-2019-11236**		010519/351
rancher					
rancher					
N/A	10-04-2019	6.5	In Rancher 2.0.0 through 2.1.5, project members have continued access to create, update, read, and delete namespaces in a project after they have been removed from it. **CVE ID : CVE-2019-6287**	https://rancher.com/blog/2019/2019-01-29-explaining-security-vulnerabilities-addressed-in-rancher-v2-1-6-and-v2-0-11/	A-RAN-RANC-010519/352
Rapid7					
insightvm					
N/A	09-04-2019	3.5	Users with Site-level permissions can access files containing the username-encrypted passwords of Security Console Global Administrators and clear-text passwords for restoring backups, as well as the salt for those passwords. Valid credentials are required to access these files and malicious users would still need to perform additional work to decrypt the credentials and escalate	https://help.rapid7.com/insightvm/en-us/release-notes/#6.5.50	A-RAP-INSI-010519/353

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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. This issue affects: Rapid7 InsightVM versions 6.5.11 through 6.5.49. **CVE ID : CVE-2019-5615**		
Redhat					
openshift_container_platform					
Improper Link Resolution Before File Access ('Link Following')	01-04-2019	5.8	The kubectl cp command allows copying files between containers and the user machine. To copy files from a container, Kubernetes creates a tar inside the container, copies it over the network, and kubectl unpacks it on the user?s machine. If the tar binary in the container is malicious, it could run any code and output unexpected, malicious results. An attacker could use this to write files to any path on the user?s machine when kubectl cp is called, limited only by the system permissions of the local user. The untar function can both create and follow symbolic links. The issue is resolved in kubectl v1.11.9, v1.12.7, v1.13.5, and v1.14.0. **CVE ID : CVE-2019-1002101**	N/A	A-RED-OPEN-010519/354
Improper Neutralizatio	01-04-2019	4.3	A flaw was found in the /oauth/token/request	https://bugzilla.redhat.co	A-RED-OPEN-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			custom endpoint of the OpenShift OAuth server allowing for XSS generation of CLI tokens due to missing X-Frame-Options and CSRF protections. If not otherwise prevented, a separate XSS vulnerability via JavaScript could further allow for the extraction of these tokens. **CVE ID : CVE-2019-3876**	m/show_bug.cgi?id=CVE-2019-3876	010519/355
satellite					
Improper Access Control	11-04-2019	5.2	A lack of access control was found in the message queues maintained by Satellite's QPID broker and used by katello-agent in versions before Satellite 6.2, Satellite 6.1 optional and Satellite Capsule 6.1. A malicious user authenticated to a host registered to Satellite (or Capsule) can use this flaw to access QMF methods to any host also registered to Satellite (or Capsule) and execute privileged commands. **CVE ID : CVE-2019-3845**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3845	A-RED-SATE-010519/356
N/A	15-04-2019	2.1	It was discovered that a world-readable log file belonging to Candlepin component of Red Hat Satellite 6.4 leaked the	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3891	A-RED-SATE-010519/357

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials of the Candlepin database. A malicious user with local access to a Satellite host can use those credentials to modify the database and prevent Satellite from fetching package updates, thus preventing all Satellite hosts from accessing those updates. **CVE ID : CVE-2019-3891**		
Information Exposure	09-04-2019	4	In Foreman it was discovered that the delete compute resource operation, when executed from the Foreman API, leads to the disclosure of the plaintext password or token for the affected compute resource. A malicious user with the "delete_compute_resource " permission can use this flaw to take control over compute resources managed by foreman. Versions before 1.20.3, 1.21.1, 1.22.0 are vulnerable. **CVE ID : CVE-2019-3893**	N/A	A-RED-SATE-010519/358
gluster_storage					
Improper Limitation of a Pathname to a Restricted	09-04-2019	5.5	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An	N/A	A-RED-GLUS-010519/359

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable. **CVE ID : CVE-2019-3880**		
libvirt					
Information Exposure	04-04-2019	4.8	An incorrect permissions check was discovered in libvirt 4.8.0 and above. The readonly permission was allowed to invoke APIs depending on the guest agent, which could lead to potentially disclosing unintended information or denial of service by causing libvirt to block. **CVE ID : CVE-2019-3886**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3886	A-RED-LIBV-010519/360
enterprise_mrg					
Information Exposure	11-04-2019	3.3	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3459**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3459.html	A-RED-ENTE-010519/361
Rockwellautomation					
rslinx					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	04-04-2019	7.5	A vulnerability was found in Rockwell Automation RSLinx Classic versions 4.10.00 and prior. An input validation issue in a .dll file of RSLinx Classic where the data in a Forward Open service request is passed to a fixed size buffer, allowing an attacker to exploit a stack-based buffer overflow condition. **CVE ID : CVE-2019-6553**	N/A	A-ROC-RSLI-010519/362
Roundcube					
webmail					
Inadequate Encryption Strength	07-04-2019	4.3	In Roundcube Webmail 1.3.4, an attacker in possession of S/MIME or PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, they unknowingly leak the plaintext of the encrypted message part(s) back to the attacker. **CVE ID : CVE-2019-10740**	N/A	A-ROU-WEBM-010519/363

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Roundup-tracker					
roundup					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2019	4.3	Roundup 1.6 allows XSS via the URI because frontends/roundup.cgi and roundup/cgi/wsgi_handler.py mishandle 404 errors. **CVE ID : CVE-2019-10904**	N/A	A-ROU-ROUN-010519/364
roxyfileman					
roxy_fileman					
Improper Input Validation	09-04-2019	7.5	Roxy Fileman 1.4.5 allows attackers to execute renamefile.php (aka Rename File), createdir.php (aka Create Directory), fileslist.php (aka Echo File List), and movefile.php (aka Move File) operations. **CVE ID : CVE-2019-7174**	N/A	A-ROX-ROXY-010519/365
salesagility					
suitecrm					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2019	7.5	SuiteCRM before 7.8.28, 7.9.x and 7.10.x before 7.10.15, and 7.11.x before 7.11.3 allows SQL Injection. **CVE ID : CVE-2019-6506**	https://suitecrm.com/suitecrm-7-11-3-lts-security-maintenance-patch-released/	A-SAL-SUIT-010519/366
Samba					
samba					

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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	09-04-2019	3.6	A vulnerability was found in Samba from version (including) 4.9 to versions before 4.9.6 and 4.10.2. During the creation of a new Samba AD DC, files are created in a private subdirectory of the install location. This directory is typically mode 0700, that is owner (root) only access. However in some upgraded installations it will have other permissions, such as 0755, because this was the default before Samba 4.8. Within this directory, files are created with mode 0666, which is world-writable, including a sample krb5.conf, and the list of DNS names and servicePrincipalName values to update. **CVE ID : CVE-2019-3870**	N/A	A-SAM-SAMB-010519/367
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2019	5.5	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba	N/A	A-SAM-SAMB-010519/368

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable. **CVE ID : CVE-2019-3880**		
SAP					
netweaver_process_integration					
Information Exposure	10-04-2019	4	Under certain conditions the Monitoring Servlet of the SAP NetWeaver Process Integration (Messaging System), fixed in versions 7.10 to 7.11, 7.20, 7.30, 7.31, 7.40, 7.50, allows an attacker to see the names of database tables used by the application, leading to information disclosure. **CVE ID : CVE-2019-0278**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=517899114	A-SAP-NETW-010519/369
Information Exposure	10-04-2019	5	Several web pages in SAP NetWeaver Process Integration (Runtime Workbench), fixed in versions 7.10 to 7.11, 7.30, 7.31, 7.40, 7.50; can be accessed without user authentication, which might expose internal data like release information, Java package and Java object names which can be misused by the attacker. **CVE ID : CVE-2019-0282**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=517899114	A-SAP-NETW-010519/370
Improper Access Control	10-04-2019	5.5	SAP NetWeaver Process Integration (Adapter Engine), fixed in versions	https://wiki.scn.sap.com/wiki/pages/	A-SAP-NETW-010519/371

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
			7.10 to 7.11, 7.30, 7.31, 7.40, 7.50; is vulnerable to Digital Signature Spoofing. It is possible to spoof XML signatures and send arbitrary requests to the server via PI Axis adapter. These requests will be accepted by the PI Axis adapter even if the payload has been altered, especially when the signed element is the body of the xml document. **CVE ID : CVE-2019-0283**	viewpage.action?pageId=517899114	
hana					
Improper Restriction of XML External Entity Reference ('XXE')	10-04-2019	3.6	SLD Registration in SAP HANA (fixed in versions 1.0, 2.0) does not sufficiently validate an XML document accepted from an untrusted source. The attacker can call SLDREG with an XML file containing a reference to an XML External Entity (XXE). This can cause SLDREG to, for example, continuously loop, read arbitrary files and even send local files. **CVE ID : CVE-2019-0284**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=517899114	A-SAP-HANA-010519/372
crystal_reports					
Information Exposure	10-04-2019	5	The .NET SDK WebForm Viewer in SAP Crystal Reports for Visual Studio (fixed in version 2010)	https://wiki.scn.sap.com/wiki/pages/viewpage.act	A-SAP-CRYS-010519/373

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discloses sensitive database information including credentials which can be misused by the attacker. **CVE ID : CVE-2019-0285**	ion?pageId=517899114	
business_application_software_integrated_solution					
Improper Authorization	10-04-2019	6.5	ABAP BASIS function modules INST_CREATE_R3_RFC_DEST, INST_CREATE_TCPIP_RFC DEST, and INST_CREATE_TCPIP_RFC_DEST in SAP BASIS (fixed in versions 7.0 to 7.02, 7.10 to 7.30, 7.31, 7.40, 7.50 to 7.53) do not perform necessary authorization checks in all circumstances for an authenticated user, resulting in escalation of privileges. **CVE ID : CVE-2019-0279**	https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=517899114	A-SAP-BUSI-010519/374
S-cms					
S-cms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2019	7.5	S-CMS PHP v1.0 has SQL injection via the 4/js/scms.php?action=unlike id parameter. **CVE ID : CVE-2019-10708**	N/A	A-S-C-S-CM-010519/375

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Silverstripe					
silverstripe					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	11-04-2019	7.5	All versions of SilverStripe 3 prior to 3.6.7 and 3.7.3, and all versions of SilverStripe 4 prior to 4.0.7, 4.1.5, 4.2.4, and 4.3.1 allows Reflected SQL Injection through Form and DataObject. **CVE ID : CVE-2019-5715**	N/A	A-SIL-SILV-010519/376
solideos					
architectural_information_system					
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.5	Architectural Information System 1.0 and earlier versions have a Stack-based buffer overflow, allows remote attackers to execute arbitrary code. **CVE ID : CVE-2019-9134**	N/A	A-SOL-ARCH-010519/377
Sony					
neural_network_libraries					
Improper Input Validation	04-04-2019	7.5	nbla/logger.cpp in libnnabla.a in Sony Neural Network Libraries (aka nnabla) through v1.0.14 relies on the HOME environment variable, which might be untrusted. **CVE ID : CVE-2019-10844**	N/A	A-SON-NEUR-010519/378
Spip					
spip					
Improper	10-04-2019	6.5	SPIP 3.1 before 3.1.10 and	N/A	A-SPI-SPIP-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			3.2 before 3.2.4 allows authenticated visitors to execute arbitrary code on the host server because var_memotri is mishandled. **CVE ID : CVE-2019-11071**		010519/379
Symantec					
vip_enterprise_gateway					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	Symantec VIP Enterprise Gateway (all versions) may be susceptible to a cross-site scripting (XSS) exploit, which is a type of issue that can enable attackers to inject client-side scripts into web pages viewed by other users. A cross-site scripting vulnerability may be used by attackers to potentially bypass access controls such as the same-origin policy. **CVE ID : CVE-2019-9696**	https://support.symantec.com/en_US/article.SYMSA1477.html	A-SYM-VIP_-010519/380
endpoint_encryption					
N/A	10-04-2019	4.6	Symantec Endpoint Encryption prior to SEE 11.2.1 MP1 may be susceptible to a Privilege Escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to	https://support.symantec.com/en_US/article.SYMSA1478.html	A-SYM-ENDP-010519/381

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources that are normally protected from an application or user. **CVE ID : CVE-2019-9694**		
systemd_project					
systemd					
N/A	09-04-2019	4.4	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It is possible for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the "allow_active" element rather than "allow_any". **CVE ID : CVE-2019-3842**	N/A	A-SYS-SYST-010519/382
Teeworlds					
teeworlds					
Integer Overflow or Wraparound	05-04-2019	7.5	In Teeworlds 0.7.2, there is an integer overflow in CMap::Load() in engine/shared/map.cpp that can lead to a buffer overflow, because multiplication of width and height is mishandled. **CVE ID : CVE-2019-10877**	N/A	A-TEE-TEEW-010519/383
Out-of-	05-04-2019	7.5	In Teeworlds 0.7.2, there is	N/A	A-TEE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			a failed bounds check in CDataFileReader::GetData() and CDataFileReader::ReplaceData() and related functions in engine/shared/datafile.cpp that can lead to an arbitrary free and out-of-bounds pointer write, possibly resulting in remote code execution. **CVE ID : CVE-2019-10878**		TEEW-010519/384
Integer Overflow or Wraparound	05-04-2019	7.5	In Teeworlds 0.7.2, there is an integer overflow in CDataFileReader::Open() in engine/shared/datafile.cpp that can lead to a buffer overflow and possibly remote code execution, because size-related multiplications are mishandled. **CVE ID : CVE-2019-10879**	N/A	A-TEE-TEEW-010519/385
Theforeman					
foreman					
Information Exposure	09-04-2019	4	In Foreman it was discovered that the delete compute resource operation, when executed from the Foreman API, leads to the disclosure of the plaintext password or token for the affected compute resource. A malicious user with the	N/A	A-THE-FORE-010519/386

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"delete_compute_resource " permission can use this flaw to take control over compute resources managed by foreman. Versions before 1.20.3, 1.21.1, 1.22.0 are vulnerable. **CVE ID : CVE-2019-3893**		
Tibco					
activematrix_businessworks					
Improper Authenticati on	09-04-2019	6.8	The HTTP Connector component of TIBCO Software Inc.'s TIBCO ActiveMatrix BusinessWorks contains a vulnerability that theoretically allows unauthenticated HTTP requests to be processed by the BusinessWorks engine even when authentication is required. This possibility is restricted to circumstances where HTTP "Basic Authentication" policy is used in conjunction with an XML Authentication resource. The BusinessWorks engine might instead use credentials from a prior HTTP request for authorization purposes. Affected releases are	N/A	A-TIB-ACTI-010519/387

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TIBCO Software Inc. TIBCO ActiveMatrix BusinessWorks: versions up to and including 6.4.2. **CVE ID : CVE-2019-8990**		
tongda2000					
office_anywhere					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-04-2019	7.5	An issue was discovered in TONGDA Office Anywhere 10.18.190121. There is a SQL Injection vulnerability via the general/approve_center/list/input_form/work_handle.php run_id parameter. **CVE ID : CVE-2019-9759**	N/A	A-TON-OFFI-010519/388
Trendmicro					
apex_one					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-04-2019	5	A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (versions XG and 11.0), and Worry-Free Business Security (versions 10.0, 9.5 and 9.0) could allow an attacker to modify arbitrary files on the affected product's management console. **CVE ID : CVE-2019-9489**	https://success.trendmicro.com/solution/1122250	A-TRE-APEX-010519/389
business_security					
Improper Limitation of a Pathname to a	05-04-2019	5	A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (versions XG	https://success.trendmicro.com/solution/1122250	A-TRE-BUSI-010519/390

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
Restricted Directory ('Path Traversal')			and 11.0), and Worry-Free Business Security (versions 10.0, 9.5 and 9.0) could allow an attacker to modify arbitrary files on the affected product's management console. **CVE ID : CVE-2019-9489**		
officescan					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	05-04-2019	5	A directory traversal vulnerability in Trend Micro Apex One, OfficeScan (versions XG and 11.0), and Worry-Free Business Security (versions 10.0, 9.5 and 9.0) could allow an attacker to modify arbitrary files on the affected product's management console. **CVE ID : CVE-2019-9489**	https://success.trendmicro.com/solution/1122250	A-TRE-OFFI-010519/391
interscan_web_security_virtual_appliance					
N/A	05-04-2019	4	A vulnerability in Trend Micro InterScan Web Security Virtual Appliance version 6.5 SP2 could allow an non-authorized user to disclose administrative credentials. An attacker must be an authenticated user in order to exploit the vulnerability. **CVE ID : CVE-2019-9490**	https://success.trendmicro.com/solution/1122326	A-TRE-INTE-010519/392
trojita_project					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
trojita					
Inadequate Encryption Strength	07-04-2019	4.3	In KDE Trojita 0.7, an attacker in possession of S/MIME or PGP encrypted emails can wrap them as sub-parts within a crafted multipart email. The encrypted part(s) can further be hidden using HTML/CSS or ASCII newline characters. This modified multipart email can be re-sent by the attacker to the intended receiver. If the receiver replies to this (benign looking) email, they unknowingly leak the plaintext of the encrypted message part(s) back to the attacker. **CVE ID : CVE-2019-10734**	N/A	A-TRO-TROJ-010519/393
Tryton					
tryton					
Improper Access Control	04-04-2019	4	In trytond/model/modelstorage.py in Tryton 4.2 before 4.2.21, 4.4 before 4.4.19, 4.6 before 4.6.14, 4.8 before 4.8.10, and 5.0 before 5.0.6, an authenticated user can order records based on a field for which he has no access right. This may allow the user to guess values.	N/A	A-TRY-TRYT-010519/394

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-10868		
ui					
edgeswitch_x					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-04-2019	9	In Ubiquiti Networks EdgeSwitch X v1.1.0 and prior, a privileged user can execute arbitrary shell commands over the SSH CLI interface. This allows to execute shell commands under the root user. **CVE ID : CVE-2019-5424**	N/A	A-UI-EDGE-010519/395
Improper Neutralization of Special Elements used in a Command ('Command Injection')	10-04-2019	9	In Ubiquiti Networks EdgeSwitch X v1.1.0 and prior, an authenticated user can execute arbitrary shell commands over the SSH interface bypassing the CLI interface, which allow them to escalate privileges to root. **CVE ID : CVE-2019-5425**	N/A	A-UI-EDGE-010519/396
Improper Access Control	10-04-2019	5.8	In Ubiquiti Networks EdgeSwitch X v1.1.0 and prior, an unauthenticated user can use the "local port forwarding" and "dynamic port forwarding" (SOCKS proxy) functionalities. Remote attackers without credentials can exploit this bug to access local services or forward traffic through the device if SSH is enabled in the system settings. **CVE ID : CVE-2019-5426**	N/A	A-UI-EDGE-010519/397

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ukcms					
ukcms					
Cross-Site Request Forgery (CSRF)	05-04-2019	6.8	A CSRF Issue that can add an admin user was discovered in UKcms v1.1.10 via admin.php/admin/role/add.html. **CVE ID : CVE-2019-10888**	N/A	A-UKC-UKCM-010519/398
ultimatemember					
ultimate_member					
Cross-Site Request Forgery (CSRF)	03-04-2019	9.3	A CSRF vulnerability in a logged-in user's profile edit form in the Ultimate Member plugin before 2.0.40 for WordPress allows attackers to become admin and subsequently extract sensitive information and execute arbitrary code. This occurs because the attacker can change the e-mail address in the administrator profile, and then the attacker is able to reset the administrator password using the WordPress "password forget" form. **CVE ID : CVE-2019-10673**	N/A	A-ULT-ULTI-010519/399
uniqkey					
password_manager					
Information Exposure	08-04-2019	4.3	An issue was discovered in Uniqkey Password Manager 1.14. Upon	N/A	A-UNI-PASS-010519/400

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			entering new credentials to a site that is not registered within this product, a pop-up window will appear prompting the user if they want to save this new password. This pop-up window will persist on any page the user enters within the browser until a decision is made. The code of the pop-up window can be read by remote servers and contains the login credentials and URL in cleartext. A malicious server could easily grab this information from the pop-up. This is related to id="uniqkey-password-popup" and password-popup/popup.html. **CVE ID : CVE-2019-10676**		
Information Exposure	08-04-2019	4.3	An issue was discovered in Uniqkey Password Manager 1.14. When entering new credentials to a site that isn't registered within this product, a pop-up window will appear asking the user if they want to save these new credentials. The code of the pop-up window can be read and, to some extent, manipulated by remote servers. This pop-	N/A	A-UNI-PASS-010519/401

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			up window will stay on any page the user visits within the browser until a decision is made. A malicious web server can forcefully manipulate the pop-up and cause it not to appear, stopping users from securing their credentials. This vulnerability is related to id="uniqkey-password-popup" and password-popup/popup.html, but is a different vulnerability than CVE-2019-10676. **CVE ID : CVE-2019-10845**		
N/A	05-04-2019	4.3	Uniqkey Password Manager 1.14 contains a vulnerability because it fails to recognize the difference between domains and sub-domains. The vulnerability means that passwords saved for example.com will be recommended for usersite.example.com. This could lead to successful phishing campaigns and create a sense of false security. **CVE ID : CVE-2019-10884**	N/A	A-UNI-PASS-010519/402
Vmware					
vcloud_director					
Session	01-04-2019	7.5	VMware vCloud Director for Service Providers 9.5.x	https://www.vmware.co	A-VMW-VCLO-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Fixation			prior to 9.5.0.3 update resolves a Remote Session Hijack vulnerability in the Tenant and Provider Portals. Successful exploitation of this issue may allow a malicious actor to access the Tenant or Provider Portals by impersonating a currently logged in session. **CVE ID : CVE-2019-5523**	m/security/advisories/VMSA-2019-0004.html	010519/403
vpcsbd					
integrated_university_management_system					
Improper Authentication	11-04-2019	10	An authentication bypass vulnerability in all versions of ValuePLUS Integrated University Management System (IUMS) allows unauthenticated, remote attackers to gain administrator privileges via the Teachers Web Panel (TWP) User ID or Password field. If exploited, the attackers could perform any actions with administrator privileges (e.g., enumerate/delete all the students' personal information or modify various settings). **CVE ID : CVE-2019-11196**	N/A	A-VPC-INTE-010519/404
vstarcam					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eye4					
Improper Input Validation	08-04-2019	10	The VStarCam vstc.vscam.client library and vstc.vscam shared object, as used in the Eye4 application (for Android, iOS, and Windows), do not prevent spoofing of the camera server. An attacker can create a fake camera server that listens for the client looking for a camera on the local network. When the camera responds to the client, it responds via the broadcast address, giving all information necessary to impersonate the camera. The attacker then floods the client with responses, causing the original camera to be denied service from the client, and thus causing the client to then communicate exclusively with the attacker's fake camera server. When connecting to the fake camera server, the client sends all details necessary to login to the camera (username and password). **CVE ID : CVE-2019-11014**	N/A	A-VST-EYE4-010519/405
Webkitgtk					
webkitgtk					

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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	10-04-2019	5	WebKitGTK and WPE WebKit prior to version 2.24.1 failed to properly apply configured HTTP proxy settings when downloading livestream video (HLS, DASH, or Smooth Streaming), an error resulting in deanonymization. This issue was corrected by changing the way livestreams are downloaded. **CVE ID : CVE-2019-11070**	N/A	A-WEB-WEBK-010519/406
Wireshark					
wireshark					
N/A	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the GSS-API dissector could crash. This was addressed in epan/dissectors/packet-gssapi.c by ensuring that a valid dissector is called. **CVE ID : CVE-2019-10894**	N/A	A-WIR-WIRE-010519/407
Improper Input Validation	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the NetScaler file parser could crash. This was addressed in wiretap/netscaler.c by improving data validation. **CVE ID : CVE-2019-10895**	N/A	A-WIR-WIRE-010519/408
N/A	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and	N/A	A-WIR-WIRE-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.0.0, the DOF dissector could crash. This was addressed in epan/dissectors/packet-dof.c by properly handling generated IID and OID bytes. **CVE ID : CVE-2019-10896**		010519/409
N/A	09-04-2019	5	In Wireshark 3.0.0, the IEEE 802.11 dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-ieee80211.c by detecting cases in which the bit offset does not advance. **CVE ID : CVE-2019-10897**	N/A	A-WIR-WIRE-010519/410
N/A	09-04-2019	5	In Wireshark 3.0.0, the GSUP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gsm_gsup.c by rejecting an invalid Information Element length. **CVE ID : CVE-2019-10898**	N/A	A-WIR-WIRE-010519/411
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the SRVLOC dissector could crash. This was addressed in epan/dissectors/packet-srvloc.c by preventing a heap-based buffer under-read.	N/A	A-WIR-WIRE-010519/412

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10899		
N/A	09-04-2019	5	In Wireshark 3.0.0, the Rbm dissector could go into an infinite loop. This was addressed in epan/dissectors/file-rbm.c by handling unknown object types safely. **CVE ID : CVE-2019-10900**	N/A	A-WIR-WIRE-010519/413
NULL Pointer Dereference	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by handling file digests properly. **CVE ID : CVE-2019-10901**	N/A	A-WIR-WIRE-010519/414
N/A	09-04-2019	5	In Wireshark 3.0.0, the TSDNS dissector could crash. This was addressed in epan/dissectors/packet-tsdns.c by splitting strings safely. **CVE ID : CVE-2019-10902**	N/A	A-WIR-WIRE-010519/415
N/A	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the DCERPC SPOOLSS dissector could crash. This was addressed in epan/dissectors/packet-dcerpc-spoolss.c by adding a boundary check. **CVE ID : CVE-2019-10903**	N/A	A-WIR-WIRE-010519/416

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wpape					
ape_gallery					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	The wpape APE GALLERY plugin 1.6.14 for WordPress has stored XSS via the classGallery.php getCategories function. **CVE ID : CVE-2019-6117**	N/A	A-WPA-APE_-010519/417
Xmlsoft					
libxslt					
Improper Access Control	10-04-2019	7.5	libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded. **CVE ID : CVE-2019-11068**	N/A	A-XML-LIBX-010519/418
xmltooling_project					
xmltooling					
Improper Input Validation	11-04-2019	5	The XMLTooling library all versions prior to V3.0.4, provided with the OpenSAML and Shibboleth Service Provider software, contains an XML parsing class. Invalid data in the XML declaration causes an exception of a type that	N/A	A-XML-XMLT-010519/419

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			was not handled properly in the parser class and propagates an unexpected exception type. **CVE ID : CVE-2019-9628**		
Zarafa					
Webaccess					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	11-04-2019	4.3	Unauthenticated reflected cross-site scripting (XSS) exists in Zarafa Webapp 2.0.1.47791 and earlier. NOTE: this is a discontinued product. The issue was fixed in later Zarafa Webapp versions; however, some former Zarafa Webapp customers use the related Kopano product instead. **CVE ID : CVE-2019-7219**	N/A	A-ZAR-WEBA-010519/420
Zohocorp					
manageengine_servicedesk_plus					
Information Exposure	04-04-2019	4	Information leakage vulnerability in the /mc login page in ManageEngine ServiceDesk Plus 9.3 software allows authenticated users to enumerate active users. Due to a flaw within the way the authentication is handled, an attacker is able to login and verify any active account.	N/A	A-ZOH-MANA-010519/421

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2019-10273		
Operating System					
Canonical					
ubuntu_linux					
N/A	08-04-2019	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **CVE ID : CVE-2019-0211**	N/A	O-CAN-UBUN-010519/422
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**	N/A	O-CAN-UBUN-010519/423
N/A	08-04-2019	1.9	A security feature bypass exists in Azure SSH Keypairs, due to a change in the provisioning logic	https://portal.msrc.microsoft.com/en-US/security-	O-CAN-UBUN-010519/424

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for some Linux images that use cloud-init, aka 'Azure SSH Keypairs Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0816**	guidance/advisory/CVE-2019-0816	
Improper Access Control	10-04-2019	7.5	libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded. **CVE ID : CVE-2019-11068**	N/A	O-CAN-UBUN-010519/425
Information Exposure	11-04-2019	3.3	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3459**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3459.html	O-CAN-UBUN-010519/426
Information Exposure	11-04-2019	3.3	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3460**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3460.html	O-CAN-UBUN-010519/427
Use After	01-04-2019	7.2	In the Linux Kernel before	N/A	O-CAN-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			versions 4.20.8 and 4.19.21 a use-after-free error in the "sctp_sendmsg()" function (net/sctp/socket.c) when handling SCTP_SENDALL flag can be exploited to corrupt memory. **CVE ID : CVE-2019-8956**		UBUN-010519/428
Improper Input Validation	11-04-2019	5	The XMLTooling library all versions prior to V3.0.4, provided with the OpenSAML and Shibboleth Service Provider software, contains an XML parsing class. Invalid data in the XML declaration causes an exception of a type that was not handled properly in the parser class and propagates an unexpected exception type. **CVE ID : CVE-2019-9628**	N/A	O-CAN-UBUN-010519/429
capsuletech					
smartlinx_neuron_2_firmware					
Improper Input Validation	11-04-2019	7.2	A restricted environment escape vulnerability exists in the "kiosk mode" function of Capsule Technologies SmartLinx Neuron 2 medical information collection devices running version 6.9.1. A specific series of keyboard inputs can escape the restricted environment, resulting in	N/A	O-CAP-SMAR-010519/430

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			full administrator access to the underlying operating system. An attacker can connect to the device via USB port with a keyboard or other HID device to trigger this vulnerability. **CVE ID : CVE-2019-5024**		
centos-webpanel					
centos_web_panel					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	03-04-2019	3.5	CentOS Web Panel (CWP) 0.9.8.789 is vulnerable to Stored/Persistent XSS for the "Name Server 1" and "Name Server 2" fields via a "DNS Functions" "Edit Nameservers IPs" action. **CVE ID : CVE-2019-10261**	N/A	O-CEN-CENT-010519/431
dasannetworks					
h660rm_firmware					
Improper Authorization	11-04-2019	6.4	diag_tool.cgi on DASAN H660RM GPON routers with firmware 1.03-0022 lacks any authorization check, which allows remote attackers to run a ping command via a GET request to enumerate LAN devices or crash the router with a DoS attack. **CVE ID : CVE-2019-9974**	N/A	O-DAS-H660-010519/432
Use of Hard-coded Credentials	11-04-2019	5	DASAN H660RM devices with firmware 1.03-0022 use a hard-coded key for logs encryption. Data	N/A	O-DAS-H660-010519/433

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stored using this key can be decrypted by anyone able to access this key. **CVE ID : CVE-2019-9975**		
N/A	11-04-2019	4	The Boa server configuration on DASAN H660RM devices with firmware 1.03-0022 logs POST data to the /tmp/boa-temp file, which allows logged-in users to read the credentials of administration web interface users. **CVE ID : CVE-2019-9976**	N/A	O-DAS-H660-010519/434
Debian					
debian_linux					
N/A	08-04-2019	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **CVE ID : CVE-2019-0211**	N/A	O-DEB-DEBI-010519/435
Concurrent Execution using Shared	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in	N/A	O-DEB-DEBI-010519/436

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**		
Improper Access Control	04-04-2019	4	In trytond/model/modelstorage.py in Tryton 4.2 before 4.2.21, 4.4 before 4.4.19, 4.6 before 4.6.14, 4.8 before 4.8.10, and 5.0 before 5.0.6, an authenticated user can order records based on a field for which he has no access right. This may allow the user to guess values. **CVE ID : CVE-2019-10868**	N/A	O-DEB-DEBI-010519/437
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-04-2019	4.3	Roundup 1.6 allows XSS via the URI because frontends/roundup.cgi and roundup/cgi/wsgi_handler.py mishandle 404 errors. **CVE ID : CVE-2019-10904**	N/A	O-DEB-DEBI-010519/438
Improper Access Control	10-04-2019	7.5	libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit	N/A	O-DEB-DEBI-010519/439

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
			access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded. **CVE ID : CVE-2019-11068**		
Out-of-bounds Read	08-04-2019	4.3	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause a heap buffer out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1787**	N/A	O-DEB-DEBI-010519/440

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-04-2019	4.3	A vulnerability in the Object Linking & Embedding (OLE2) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for OLE2 files sent an affected device. An attacker could exploit this vulnerability by sending malformed OLE2 files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds write condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1788**	N/A	O-DEB-DEBI-010519/441
N/A	09-04-2019	4.4	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It is possible for an attacker, in some particular configurations, to set a	N/A	O-DEB-DEBI-010519/442

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
			XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the "allow_active" element rather than "allow_any". **CVE ID : CVE-2019-3842**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2019	5.5	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable. **CVE ID : CVE-2019-3880**	N/A	O-DEB-DEBI-010519/443
Fedoraproject					
fedora					
N/A	08-04-2019	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent	N/A	O-FED-FEDO-010519/444

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
			process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **CVE ID : CVE-2019-0211**		
Improper Access Control	08-04-2019	6	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions. **CVE ID : CVE-2019-0215**	N/A	O-FED-FEDO-010519/445
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**	N/A	O-FED-FEDO-010519/446
N/A	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the GSS-API dissector could crash. This was addressed in epan/dissectors/packet-gssapi.c by ensuring that a valid dissector is called. **CVE ID : CVE-2019-10894**	N/A	O-FED-FEDO-010519/447
Improper	09-04-2019	5	In Wireshark 2.4.0 to	N/A	O-FED-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the NetScaler file parser could crash. This was addressed in wiretap/netscaler.c by improving data validation. **CVE ID : CVE-2019-10895**		FEDO-010519/448
N/A	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the DOF dissector could crash. This was addressed in epan/dissectors/packet-dof.c by properly handling generated IID and OID bytes. **CVE ID : CVE-2019-10896**	N/A	O-FED-FEDO-010519/449
N/A	09-04-2019	5	In Wireshark 3.0.0, the IEEE 802.11 dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-ieee80211.c by detecting cases in which the bit offset does not advance. **CVE ID : CVE-2019-10897**	N/A	O-FED-FEDO-010519/450
N/A	09-04-2019	5	In Wireshark 3.0.0, the GSUP dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-gsm_gsup.c by rejecting an invalid Information Element length. **CVE ID : CVE-2019-10898**	N/A	O-FED-FEDO-010519/451

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the SRVLOC dissector could crash. This was addressed in epan/dissectors/packet-srvloc.c by preventing a heap-based buffer under-read. **CVE ID : CVE-2019-10899**	N/A	O-FED-FEDO-010519/452
N/A	09-04-2019	5	In Wireshark 3.0.0, the Rbm dissector could go into an infinite loop. This was addressed in epan/dissectors/file-rbm.c by handling unknown object types safely. **CVE ID : CVE-2019-10900**	N/A	O-FED-FEDO-010519/453
NULL Pointer Dereference	09-04-2019	5	In Wireshark 2.4.0 to 2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the LDSS dissector could crash. This was addressed in epan/dissectors/packet-ldss.c by handling file digests properly. **CVE ID : CVE-2019-10901**	N/A	O-FED-FEDO-010519/454
N/A	09-04-2019	5	In Wireshark 3.0.0, the TSDNS dissector could crash. This was addressed in epan/dissectors/packet-tsdns.c by splitting strings safely. **CVE ID : CVE-2019-10902**	N/A	O-FED-FEDO-010519/455
N/A	09-04-2019	5	In Wireshark 2.4.0 to	N/A	O-FED-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.4.13, 2.6.0 to 2.6.7, and 3.0.0, the DCERPC SPOOLSS dissector could crash. This was addressed in epan/dissectors/packet-dcerpc-spoolss.c by adding a boundary check. **CVE ID : CVE-2019-10903**		FEDO-010519/456
N/A	09-04-2019	4.4	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It is possible for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the "allow_active" element rather than "allow_any". **CVE ID : CVE-2019-3842**	N/A	O-FED-FEDO-010519/457
N/A	09-04-2019	3.6	A vulnerability was found in Samba from version (including) 4.9 to versions before 4.9.6 and 4.10.2. During the creation of a new Samba AD DC, files are created in a private subdirectory of the install location. This directory is typically mode 0700, that is owner (root) only	N/A	O-FED-FEDO-010519/458

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access. However in some upgraded installations it will have other permissions, such as 0755, because this was the default before Samba 4.8. Within this directory, files are created with mode 0666, which is world-writable, including a sample krb5.conf, and the list of DNS names and servicePrincipalName values to update. **CVE ID : CVE-2019-3870**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2019	5.5	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable. **CVE ID : CVE-2019-3880**	N/A	O-FED-FEDO-010519/459
Improper Neutralization of Input During Web Page Generation	08-04-2019	4.3	simple-markdown.js in Khan Academy simple-markdown before 0.4.4 allows XSS via a data: or vbscript: URI. **CVE ID : CVE-2019-9844**	N/A	O-FED-FEDO-010519/460

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
('Cross-site Scripting')					
glory-global					
rbw-100_firmware					
Unrestricted Upload of File with Dangerous Type	05-04-2019	9	An issue was discovered on Glory RBW-100 devices with firmware ISP-K05-02 7.0.0. An unrestricted file upload vulnerability in the Front Circle Controller glytoolcgi/settingfile_upload.cgi allows attackers to upload supplied data. This can be used to place attacker controlled code on the filesystem that can be executed and can lead to a reverse root shell. **CVE ID : CVE-2019-10478**	N/A	O-GLO-RBW-- 010519/461
Use of Hard-coded Credentials	05-04-2019	10	An issue was discovered on Glory RBW-100 devices with firmware ISP-K05-02 7.0.0. A hard-coded username and password were identified that allow a remote attacker to gain admin access to the Front Circle Controller web interface. **CVE ID : CVE-2019-10479**	N/A	O-GLO-RBW-- 010519/462
Juniper					
junos					
Improper Restriction of Operations	10-04-2019	7.5	A certain sequence of valid BGP or IPv6 BFD packets may trigger a stack based buffer overflow in the	https://kb.juniper.net/JSA10930	O-JUN-JUNO-010519/463

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Junos OS Packet Forwarding Engine manager (FXPC) process on QFX5000 series, EX4300, EX4600 devices. This issue can result in a crash of the fxpc daemon or may potentially lead to remote code execution. Affected releases are Juniper Networks Junos OS on QFX 5000 series, EX4300, EX4600 are: 14.1X53; 15.1X53 versions prior to 15.1X53-D235; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3; 17.3 versions prior to 17.3R3-S2, 17.3R4; 17.4 versions prior to 17.4R2-S1, 17.4R3; 18.1 versions prior to 18.1R3-S1, 18.1R4; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R2. **CVE ID : CVE-2019-0008**		
Improper Input Validation	10-04-2019	5	When BGP tracing is enabled an incoming BGP message may cause the Junos OS routing protocol daemon (rpd) process to crash and restart. While rpd restarts after a crash, repeated crashes can result in an extended DoS	https://kb.juniper.net/JSA10931	O-JUN-JUNO-010519/464

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7-S4, 16.1R7-S5; 16.2 versions prior to 16.2R2-S9, 16.2R3; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R3-S1; 17.3 versions prior to 17.3R3-S3, 17.3R3-S4, 17.3R4; 17.4 versions prior to 17.4R1-S7, 17.4R2-S3, 17.4R2-S4, 17.4R3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S4, 18.1R4; 18.2 versions prior to 18.2R2-S2, 18.2R2-S3, 18.2R3; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S3, 18.3R2; 18.4 versions prior to 18.4R1-S2, 18.4R2. This issue does not affect Junos releases prior to 16.1R1. **CVE ID : CVE-2019-0019**		
Improper Input Validation	10-04-2019	5	On Junos devices with the BGP graceful restart helper mode enabled or the BGP graceful restart mechanism enabled, a BGP session restart on a remote peer that has the graceful restart mechanism enabled may cause the local routing	https://kb.juniper.net/JSA10932	O-JUN-JUNO-010519/465

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protocol daemon (RPD) process to crash and restart. By simulating a specific BGP session restart, an attacker can repeatedly crash the RPD process causing prolonged denial of service (DoS). Graceful restart helper mode for BGP is enabled by default. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS: 16.1 versions prior to 16.1R7; 16.1X65 versions prior to 16.1X65-D48; 16.2 versions prior to 16.2R2-S8; 17.1 versions prior to 17.1R2-S7, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D92, 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R2-S2, 17.3R3; 17.4 versions prior to 17.4R1-S4, 17.4R2; 18.1 versions prior to 18.1R2. Junos OS releases prior to 16.1R1 are not affected. **CVE ID : CVE-2019-0028**		
N/A	10-04-2019	5	Specific IPv6 DHCP packets received by the jdhcpd daemon will cause	https://kb.juniper.net/JSA10920	O-JUN-JUNO-010519/466

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a memory resource consumption issue to occur on a Junos OS device using the jdhcpd daemon configured to respond to IPv6 requests. Once started, memory consumption will eventually impact any IPv4 or IPv6 request serviced by the jdhcpd daemon, thus creating a Denial of Service (DoS) condition to clients requesting and not receiving IP addresses. Additionally, some clients which were previously holding IPv6 addresses will not have their IPv6 Identity Association (IA) address and network tables agreed upon by the jdhcpd daemon after the failover event occurs, which leads to more than one interface, and multiple IP addresses, being denied on the client. Affected releases are Juniper Networks Junos OS: 17.4 versions prior to 17.4R2; 18.1 versions prior to 18.1R2. **CVE ID : CVE-2019-0031**		
Uncontrolled Resource Consumption	10-04-2019	5	A firewall bypass vulnerability in the proxy ARP service of Juniper Networks Junos OS allows	https://kb.juniper.net/JSA10922	O-JUN-JUNO-010519/467

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an attacker to cause a high CPU condition leading to a Denial of Service (DoS). This issue affects only IPv4. Affected releases are Juniper Networks Junos OS: 12.1X46 versions above and including 12.1X46-D25 prior to 12.1X46-D71, 12.1X46-D73 on SRX Series; 12.3X48 versions prior to 12.3X48-D50 on SRX Series; 15.1X49 versions prior to 15.1X49-D75 on SRX Series. **CVE ID : CVE-2019-0033**		
N/A	10-04-2019	7.2	When "set system ports console insecure" is enabled, root login is disallowed for Junos OS as expected. However, the root password can be changed using "set system root-authentication plain-text-password" on systems booted from an OAM (Operations, Administration, and Maintenance) volume, leading to a possible administrative bypass with physical access to the console. OAM volumes (e.g. flash drives) are typically instantiated as /dev/gpt/oam, or /oam for short. Password	https://kb.juniper.net/JSA10924	O-JUN-JUNO-010519/468

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
			recovery, changing the root password from a console, should not have been allowed from an insecure console. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1F6-S12, 15.1R7-S3; 15.1X49 versions prior to 15.1X49-D160; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D496, 15.1X53-D68; 16.1 versions prior to 16.1R3-S10, 16.1R6-S6, 16.1R7-S3; 16.1X65 versions prior to 16.1X65-D49; 16.2 versions prior to 16.2R2-S8; 17.1 versions prior to 17.1R2-S10, 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S3; 17.4 versions prior to 17.4R1-S6, 17.4R2-S2; 18.1 versions prior to 18.1R2-S4, 18.1R3-S3; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S2. This issue does not affect Junos OS releases prior to 15.1. **CVE ID : CVE-2019-0035**		
N/A	10-04-2019	7.5	When configuring a stateless firewall filter in	https://kb.juniper.net/JS	O-JUN-JUNO-010519/469

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS, terms named using the format "internal-n" (e.g. "internal-1", "internal-2", etc.) are silently ignored. No warning is issued during configuration, and the config is committed without error, but the filter criteria will match all packets leading to unexpected results. Affected releases are Juniper Networks Junos OS: All versions prior to and including 12.3; 14.1X53 versions prior to 14.1X53-D130, 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X49 versions prior to 15.1X49-D161, 15.1X49-D170; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D496, 15.1X53-D69; 16.1 versions prior to 16.1R7-S4, 16.1R7-S5; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S4; 17.4 versions prior to 17.4R1-S7, 17.4R2-S3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S4; 18.2 versions prior to 18.2R1-S5, 18.2R2-S1;	A10925	

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-S3; 18.4 versions prior to 18.4R1-S1, 18.4R1-S2. **CVE ID : CVE-2019-0036**		
Improper Input Validation	10-04-2019	5	In a Dynamic Host Configuration Protocol version 6 (DHCPv6) environment, the jdhcpd daemon may crash and restart upon receipt of certain DHCPv6 solicit messages received from a DHCPv6 client. By continuously sending the same crafted packet, an attacker can repeatedly crash the jdhcpd process causing a sustained Denial of Service (DoS) to both IPv4 and IPv6 clients. Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1F6-S12, 15.1R7-S3; 15.1X49 versions prior to 15.1X49-D171, 15.1X49-D180; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D496; 16.1 versions prior to 16.1R3-S10, 16.1R7-S4; 16.2 versions prior to 16.2R2-S8; 17.1 versions prior to 17.1R2-S10, 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3	https://kb.juniper.net/JSA10926	O-JUN-JUNO-010519/470

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.3R3-S3; 17.4 versions prior to 17.4R1-S6, 17.4R2-S3; 18.1 versions prior to 18.1R2-S4, 18.1R3-S2; 18.2 versions prior to 18.2R2; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R1-S2. This issue does not affect Junos OS releases prior to 15.1. **CVE ID : CVE-2019-0037**		
N/A	10-04-2019	6.1	Crafted packets destined to the management interface (fxp0) of an SRX340 or SRX345 services gateway may create a denial of service (DoS) condition due to buffer space exhaustion. This issue only affects the SRX340 and SRX345 services gateways. No other products or platforms are affected by this vulnerability. Affected releases are Juniper Networks Junos OS: 15.1X49 versions prior to 15.1X49-D160 on SRX340/SRX345; 17.3 on SRX340/SRX345; 17.4 versions prior to 17.4R2-S3, 17.4R3 on SRX340/SRX345; 18.1 versions prior to 18.1R3-S1 on SRX340/SRX345;	https://kb.juniper.net/JSA10927	O-JUN-JUNO-010519/471

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2 versions prior to 18.2R2 on SRX340/SRX345; 18.3 versions prior to 18.3R1-S2, 18.3R2 on SRX340/SRX345. This issue does not affect Junos OS releases prior to 15.1X49 on any platform. **CVE ID : CVE-2019-0038**		
N/A	10-04-2019	4.3	If REST API is enabled, the Junos OS login credentials are vulnerable to brute force attacks. The high default connection limit of the REST API may allow an attacker to brute-force passwords using advanced scripting techniques. Additionally, administrators who do not enforce a strong password policy can increase the likelihood of success from brute force attacks. Affected releases are Juniper Networks Junos OS: 14.1X53 versions prior to 14.1X53-D49; 15.1 versions prior to 15.1F6-S12, 15.1R7-S3; 15.1X49 versions prior to 15.1X49-D160; 15.1X53 versions prior to 15.1X53-D236, 15.1X53-D495, 15.1X53-D591, 15.1X53-D69; 16.1 versions prior to 16.1R3-S10, 16.1R4-S12, 16.1R6-	https://kb.juniper.net/JSA10928	O-JUN-JUNO-010519/472

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S6, 16.1R7-S3; 16.1X65 versions prior to 16.1X65-D49; 16.2 versions prior to 16.2R2-S7; 17.1 versions prior to 17.1R2-S10, 17.1R3; 17.2 versions prior to 17.2R1-S8, 17.2R3-S1; 17.3 versions prior to 17.3R3-S2; 17.4 versions prior to 17.4R1-S6, 17.4R2-S2; 18.1 versions prior to 18.1R2-S4, 18.1R3-S1; 18.2 versions prior to 18.2R1-S5; 18.2X75 versions prior to 18.2X75-D30; 18.3 versions prior to 18.3R1-S1. **CVE ID : CVE-2019-0039**		
Improper Input Validation	10-04-2019	6.4	On Junos OS, rpcbind should only be listening to port 111 on the internal routing instance (IRI). External packets destined to port 111 should be dropped. Due to an information leak vulnerability, responses were being generated from the source address of the management interface (e.g. fxp0) thus disclosing internal addressing and existence of the management interface itself. A high rate of crafted packets destined to port 111 may also lead to a	https://kb.juniper.net/JSA10929	O-JUN-JUNO-010519/473

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
			partial Denial of Service (DoS). Note: Systems with fxp0 disabled or unconfigured are not vulnerable to this issue. This issue only affects Junos OS releases based on FreeBSD 10 or higher (typically Junos OS 15.1+). Administrators can confirm whether systems are running a version of Junos OS based on FreeBSD 10 or higher by typing: user@junos> show version | match kernel JUNOS OS Kernel 64-bit [20181214.223829_fbsd-builder_stable_10] Affected releases are Juniper Networks Junos OS: 15.1 versions prior to 15.1F6-S12, 15.1R7-S4; 15.1X53 versions prior to 15.1X53-D236; 16.1 versions prior to 16.1R7-S1; 16.2 versions prior to 16.2R2-S9; 17.1 versions prior to 17.1R3; 17.2 versions prior to 17.2R1-S8; 17.3 versions prior to 17.3R2; 17.4 versions prior to 17.4R1-S1, 17.4R1-S7, 17.4R2. This issue does not affect Junos OS releases prior to 15.1. **CVE ID : CVE-2019-0040**		
N/A	10-04-2019	5	On EX4300-MP Series	https://kb.ju	O-JUN-JUNO-

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices with any lo0 filters applied, transit network traffic may reach the control plane via loopback interface (lo0). The device may fail to forward such traffic. This issue affects Juniper Networks Junos OS 18.2 versions prior to 18.2R1-S2, 18.2R2 on EX4300-MP Series. This issue does not affect any other EX series devices. **CVE ID : CVE-2019-0041**	niper.net/JSA10933	010519/474
Improper Input Validation	10-04-2019	5	In MPLS environments, receipt of a specific SNMP packet may cause the routing protocol daemon (RPD) process to crash and restart. By continuously sending a specially crafted SNMP packet, an attacker can repetitively crash the RPD process causing prolonged denial of service. No other Juniper Networks products or platforms are affected by this issue. Affected releases are Juniper Networks Junos OS : 12.1X46 versions prior to 12.1X46-D77 on SRX Series; 12.3 versions prior to 12.3R12-S10; 12.3X48 versions prior to 12.3X48-D75 on SRX Series; 14.1X53 versions prior to	https://kb.juniper.net/JSA10935	O-JUN-JUNO-010519/475

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			14.1X53-D48 on EX/QFX series; 15.1 versions prior to 15.1R4-S9, 15.1R7-S2; 15.1F6 versions prior to 15.1F6-S11; 15.1X49 versions prior to 15.1X49-D141, 15.1X49-D144, 15.1X49-D150 on SRX Series; 15.1X53 versions prior to 15.1X53-D234 on QFX5200/QFX5110 Series; 15.1X53 versions prior to 15.1X53-D68 on QFX10K Series; 15.1X53 versions prior to 15.1X53-D471, 15.1X53-D490 on NFX Series; 15.1X53 versions prior to 15.1X53-D590 on EX2300/EX3400 Series; 15.1X54 on ACX Series; 16.1 versions prior to 16.1R3-S10, 16.1R4-S11, 16.1R6-S5, 16.1R7; 16.1X65 versions prior to 16.1X65-D48; 16.2 versions prior to 16.2R2-S6; 17.1 versions prior to 17.1R2-S8, 17.1R3; 17.2 versions prior to 17.2R1-S7, 17.2R3; 17.2X75 versions prior to 17.2X75-D92, 17.2X75-D102, 17.2X75-D110; 17.3 versions prior to 17.3R3; 17.4 versions prior to 17.4R1-S4, 17.4R2; 18.1 versions prior to 18.1R1-S1, 18.1R2-S1, 18.1R3; 18.2X75 versions prior to		

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75-D10. **CVE ID : CVE-2019-0043**		
Improper Input Validation	10-04-2019	5	Receipt of a specific packet on the out-of-band management interface fxp0 may cause the system to crash and restart (vmcore). By continuously sending a specially crafted packet to the fxp0 interface, an attacker can repetitively crash the rpd process causing prolonged Denial of Service (DoS). Affected releases are Juniper Networks SRX5000 Series: 12.1X46 versions prior to 12.1X46-D82; 12.3X48 versions prior to 12.3X48-D80; 15.1X49 versions prior to 15.1X49-D160. **CVE ID : CVE-2019-0044**	https://kb.juniper.net/JSA10936	O-JUN-JUNO-010519/476
Lenovo					
yangtian_afh110_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various	N/A	O-LEN-YANG-010519/477

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
yangtian_afh81_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/478
yangtian_mc_h110_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx).	N/A	O-LEN-YANG-010519/479

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
yangtian_mc_h110_pci_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/480
yangtian_mc_h81_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional	N/A	O-LEN-YANG-010519/481

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
yangtian_me/we_h110_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/482
yangtian_mf/wf_h110_pci_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to	N/A	O-LEN-YANG-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		010519/483
yangtian_mf/wf_h81_pci_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/484
yangtian_ms/ws_h81_firmware					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/485
yangtian_tc/wc_h110_pci_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which	N/A	O-LEN-YANG-010519/486

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
			keeps systems protected. **CVE ID : CVE-2019-6156**		
yangtian_tc/wcc_h81_pci_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-YANG-010519/487
yangtian_ytm6900e-00_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is	N/A	O-LEN-YANG-010519/488

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p310_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/489
thinkstation_p410_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3	N/A	O-LEN-THIN-010519/490

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
			sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p500_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/491
thinkstation_p510_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected	N/A	O-LEN-THIN-010519/492

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p520_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/493
thinkstation_p720_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient	N/A	O-LEN-THIN-010519/494

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p910_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/495
thinkcentre_x1_aio_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is	N/A	O-LEN-THIN-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		010519/496
thinkstation_c30_refresh_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/497

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkstation_d30_refresh_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/498
thinkstation_p710_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS	N/A	O-LEN-THIN-010519/499

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_s30_refresh_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/500
510-15ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for	N/A	O-LEN-510--010519/501

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
			Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
510s-08ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-510S-010519/502
530s-07icb_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that	N/A	O-LEN-530S-010519/503

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
aio520-22ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-AIO5-010519/504
aio520-22iku_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is	N/A	O-LEN-AIO5-010519/505

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
aio520-24ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-AIO5-010519/506
aio520-24iku_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this	N/A	O-LEN-AIO5-010519/507

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
			provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
aio520-27ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-AIO5-010519/508
aio_y910-27ish_firmware					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-AIO_-010519/509
h50-30g_desktop_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which	N/A	O-LEN-H50--010519/510

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
			keeps systems protected. **CVE ID : CVE-2019-6156**		
ideacentre_300-20ish_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-IDEA-010519/511
ideacentre_300s-11ish_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is	N/A	O-LEN-IDEA-010519/512

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
ideacentre_510s-08ish_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-IDEA-010519/513
ideacentre_620s-03ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3	N/A	O-LEN-IDEA-010519/514

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
			sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
legion_y520t_z370_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-LEGI-010519/515
legion_y720_tower_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected	N/A	O-LEN-LEGI-010519/516

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
legion_y920_tower_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-LEGI-010519/517
lenovo_63_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient	N/A	O-LEN-LENO-010519/518

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
m4500_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-M450-010519/519
m4500_id_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is	N/A	O-LEN-M450-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		010519/520
m4550_id_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-M455-010519/521

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qitian_4500_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-QITI-010519/522
qitian_b4550_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS	N/A	O-LEN-QITI-010519/523

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
qitian_b4650_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-QITI-010519/524
qitian_m4550_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for	N/A	O-LEN-QITI-010519/525

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
qitian_m4600_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-QITI-010519/526
qitian_m4650_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that	N/A	O-LEN-QITI-010519/527

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
qt_a7400_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-QT_A-010519/528
qt_b415_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is	N/A	O-LEN-QT_B-010519/529

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
qt_m410_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-QT_M-010519/530
qt_m415_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this	N/A	O-LEN-QT_M-010519/531

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcenter_m700z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/532
thinkcenter_m800z_firmware					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/533
thinkcentre_e73_(sff)_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which	N/A	O-LEN-THIN-010519/534

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
			keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_e73_(twr)_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/535
thinkcentre_e73s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is	N/A	O-LEN-THIN-010519/536

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_e74_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/537
thinkcentre_e74s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3	N/A	O-LEN-THIN-010519/538

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_e74z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/539
thinkcentre_e75s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected	N/A	O-LEN-THIN-010519/540

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_e75t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/541
thinkcentre_m4500k_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient	N/A	O-LEN-THIN-010519/542

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m4500q_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/543
thinkcentre_m4500s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is	N/A	O-LEN-THIN-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		010519/544
thinkcentre_m4500t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/545

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
thinkcentre_m4600s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/546
thinkcentre_m4600t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS	N/A	O-LEN-THIN-010519/547

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m700s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/548
thinkcentre_m700t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for	N/A	O-LEN-THIN-010519/549

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m700z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/550
thinkcentre_m710e_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that	N/A	O-LEN-THIN-010519/551

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m710s_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/552
thinkcentre_m710t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is	N/A	O-LEN-THIN-010519/553

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m720t_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/554
thinkcentre_m7300z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this	N/A	O-LEN-THIN-010519/555

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m73_(sff)_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/556
thinkcentre_m73_(twr)_firmware					

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/557
thinkcentre_m73_tiny_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which	N/A	O-LEN-THIN-010519/558

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m800z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/559
thinkcentre_m810z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is	N/A	O-LEN-THIN-010519/560

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m818z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/561
thinkcentre_m820z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3	N/A	O-LEN-THIN-010519/562

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
			sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m8300z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/563
thinkcentre_m8350z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected	N/A	O-LEN-THIN-010519/564

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m83z_(aio)_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/565
thinkcentre_m900z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient	N/A	O-LEN-THIN-010519/566

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkcentre_m910z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/567
thinkcentre_m920z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is	N/A	O-LEN-THIN-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		010519/568
thinkcentre_m9500z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/569

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
thinkcentre_m9550z_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/570
thinkcentre_s510_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS	N/A	O-LEN-THIN-010519/571

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p520c_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/572
thinkstation_p700_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for	N/A	O-LEN-THIN-010519/573

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
thinkstation_p900_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-THIN-010519/574
thinkstation_p920_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that	N/A	O-LEN-THIN-010519/575

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
v520s-08ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**	N/A	O-LEN-V520-010519/576
v520t-15ikl_firmware					
N/A	10-04-2019	2.1	In Lenovo systems, SMM BIOS Write Protection is used to prevent writes to SPI Flash. While this provides sufficient protection, an additional layer of protection is	N/A	O-LEN-V520-010519/577

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
			provided by SPI Protected Range Registers (PRx). Lenovo was notified that after resuming from S3 sleep mode in various versions of BIOS for Lenovo systems, the PRx is not set. This does not impact the SMM BIOS Write Protection, which keeps systems protected. **CVE ID : CVE-2019-6156**		
Linux					
linux_kernel					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	11-04-2019	4.7	The Linux kernel before 4.8 allows local users to bypass ASLR on setuid programs (such as /bin/su) because install_exec_creds() is called too late in load_elf_binary() in fs/binfmt_elf.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat. **CVE ID : CVE-2019-11190**	N/A	O-LIN-LINU-010519/578
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	11-04-2019	1.9	The Linux kernel through 5.0.7, when CONFIG_IA32_AOUT is enabled and ia32_aout is loaded, allows local users to bypass ASLR on setuid a.out programs (if any exist) because install_exec_creds() is	N/A	O-LIN-LINU-010519/579

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			called too late in load_aout_binary() in fs/binfmt_aout.c, and thus the ptrace_may_access() check has a race condition when reading /proc/pid/stat. **CVE ID : CVE-2019-11191**		
Information Exposure	11-04-2019	3.3	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3459**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3459.html	O-LIN-LINU-010519/580
Information Exposure	11-04-2019	3.3	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3460**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3460.html	O-LIN-LINU-010519/581
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-04-2019	4.9	It was found that the net_dma code in tcp_recvmsg() in the 2.6.32 kernel as shipped in RHEL6 is thread-unsafe. So an unprivileged multi-threaded userspace application calling recvmsg() for the same network socket in parallel executed on ioatdma-enabled hardware with net_dma enabled can leak	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3837	O-LIN-LINU-010519/582

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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, crash the host leading to a denial-of-service or cause a random memory corruption. **CVE ID : CVE-2019-3837**		
Improper Input Validation	09-04-2019	4.7	A flaw was found in the way KVM hypervisor handled x2APIC Machine Specific Rregister (MSR) access with nested(=1) virtualization enabled. In that, L1 guest could access L0's APIC register values via L2 guest, when 'virtualize x2APIC mode' is enabled. A guest could use this flaw to potentially crash the host kernel resulting in DoS issue. Kernel versions from 4.16 and newer are vulnerable to this issue. **CVE ID : CVE-2019-3887**	N/A	O-LIN-LINU-010519/583
Use After Free	01-04-2019	7.2	In the Linux Kernel before versions 4.20.8 and 4.19.21 a use-after-free error in the "sctp_sendmsg()" function (net/sctp/socket.c) when handling SCTP_SENDALL flag can be exploited to corrupt memory. **CVE ID : CVE-2019-8956**	N/A	O-LIN-LINU-010519/584
Microsoft					
azure_devops_server_2019					
Improper	09-04-2019	4.3	A spoofing vulnerability	N/A	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
Input Validation			that could allow a security feature bypass exists in when Azure DevOps Server does not properly sanitize user provided input, aka 'Azure DevOps Server Spoofing Vulnerability'. **CVE ID : CVE-2019-0857**		AZUR-010519/585
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0867, CVE-2019-0868, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0866**	N/A	O-MIC-AZUR-010519/586
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-AZUR-010519/587

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0866, CVE-2019-0868, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0867**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0866, CVE-2019-0867, CVE-2019-0870, CVE-2019-0871. **CVE ID : CVE-2019-0868**	N/A	O-MIC-AZUR-010519/588
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	09-04-2019	4.3	A spoofing vulnerability exists in Microsoft Azure DevOps Server when it fails to properly handle web requests, aka 'Azure DevOps Server HTML Injection Vulnerability'. **CVE ID : CVE-2019-0869**	N/A	O-MIC-AZUR-010519/589
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team	N/A	O-MIC-AZUR-010519/590

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

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

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-2019-0866, CVE-2019-0867, CVE-2019-0868, CVE-2019-0871. **CVE ID : CVE-2019-0870**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server and Team Foundation Server do not properly sanitize user provided input, aka 'Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability'. This CVE ID is unique from CVE-2019-0866, CVE-2019-0867, CVE-2019-0868, CVE-2019-0870. **CVE ID : CVE-2019-0871**	N/A	O-MIC-AZUR-010519/591
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	4.3	A Cross-site Scripting (XSS) vulnerability exists when Azure DevOps Server does not properly sanitize user provided input, aka 'Azure DevOps Server Cross-site Scripting Vulnerability'. **CVE ID : CVE-2019-0874**	N/A	O-MIC-AZUR-010519/592
N/A	09-04-2019	5	An elevation of privilege vulnerability exists when Azure DevOps Server 2019 does not properly enforce	N/A	O-MIC-AZUR-010519/593

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			project permissions, aka 'Azure DevOps Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0875**		
windows_10					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/594
Information Exposure	08-04-2019	4.3	An information disclosure vulnerability exists when the Windows GDI	https://portal.msrc.microsoft.com/en	O-MIC-WIND-010519/595

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			component improperly discloses the contents of its memory, aka 'Windows GDI Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0774. **CVE ID : CVE-2019-0614**	-US/security-guidance/advisory/CVE-2019-0614	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/596
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0689, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0682**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0682	O-MIC-WIND-010519/597
N/A	09-04-2019	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	N/A	O-MIC-WIND-010519/598

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0803, CVE-2019-0859. **CVE ID : CVE-2019-0685**		
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0688**	N/A	O-MIC-WIND-010519/599
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0689**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0689	O-MIC-WIND-010519/600
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690	O-MIC-WIND-010519/601

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
			CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**		
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0692**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0692	O-MIC-WIND-010519/602
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0694. **CVE ID : CVE-2019-0693**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0693	O-MIC-WIND-010519/603
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0694	O-MIC-WIND-010519/604

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0693. **CVE ID : CVE-2019-0694**		
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0701. **CVE ID : CVE-2019-0695**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0695	O-MIC-WIND-010519/605
N/A	08-04-2019	7.2	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-2019-0696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0696	O-MIC-WIND-010519/606
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697	O-MIC-WIND-010519/607

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0698, CVE-2019-0726. **CVE ID : CVE-2019-0697**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0726. **CVE ID : CVE-2019-0698**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0698	O-MIC-WIND-010519/608
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0695. **CVE ID : CVE-2019-0701**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0701	O-MIC-WIND-010519/609
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/610

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
			CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**		
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/611
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/612
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0698.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726	O-MIC-WIND-010519/613

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
			CVE ID : CVE-2019-0726		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/614
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0731**	N/A	O-MIC-WIND-010519/615
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'.	N/A	O-MIC-WIND-010519/616

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0732		
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/617
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/618
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755	O-MIC-WIND-010519/619
Improper Restriction of XML External	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010519/620

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	guidance/advisory/CVE-2019-0756	
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/621
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/622
N/A	08-04-2019	7.2	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0766	O-MIC-WIND-010519/623
Information Exposure	08-04-2019	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 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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0767	010519/624
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/625
Information Exposure	08-04-2019	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-2019-0614.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/626

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
			CVE ID : CVE-2019-0774		
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/627
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0776**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0776	O-MIC-WIND-010519/628
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/629
Improper	08-04-2019	7.6	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
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	WIND-010519/630
N/A	09-04-2019	7.5	An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine, aka 'SMB Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0786**	N/A	O-MIC-WIND-010519/631
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**	N/A	O-MIC-WIND-010519/632
Improper Restriction of XML External Entity	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka	N/A	O-MIC-WIND-010519/633

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reference ('XXE')			'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**		
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/634
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**	N/A	O-MIC-WIND-010519/635
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure	N/A	O-MIC-WIND-010519/636

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0837**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/637
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/638
Information Exposure	09-04-2019	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-2019-0844. **CVE ID : CVE-2019-0840**	N/A	O-MIC-WIND-010519/639
N/A	09-04-2019	7.2	An elevation of privilege	N/A	O-MIC-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836. **CVE ID : CVE-2019-0841**		WIND-010519/640
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**	N/A	O-MIC-WIND-010519/641
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/642

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/643
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/644
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**	N/A	O-MIC-WIND-010519/645
N/A	08-04-2019	7.2	An elevation of privilege vulnerability exists in Windows when the	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
			Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	-US/security-guidance/advisory/CVE-2019-0797	010519/646
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/647
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**	N/A	O-MIC-WIND-010519/648
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-010519/649

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0848. **CVE ID : CVE-2019-0814**	N/A	O-MIC-WIND-010519/650
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/651
Information Exposure	09-04-2019	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-2019-0840. **CVE ID : CVE-2019-0844**	N/A	O-MIC-WIND-010519/652

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**	N/A	O-MIC-WIND-010519/653
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/654
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**	N/A	O-MIC-WIND-010519/655
Information	09-04-2019	2.1	An information disclosure vulnerability exists when	N/A	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
Exposure			the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**		010519/656
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/657
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/658
Improper Restriction of Operations within the	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in	N/A	O-MIC-WIND-010519/659

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
Bounds of a Memory Buffer			the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0853**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/660
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/661
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/662

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/663
windows_7					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/664

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/665
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/666
N/A	08-04-2019	4.3	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0683	O-MIC-WIND-010519/667

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0683		
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690	O-MIC-WIND-010519/668
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/669
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/670

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**		
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/671
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/672
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836,	N/A	O-MIC-WIND-010519/673

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0841. **CVE ID : CVE-2019-0731**		
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**	N/A	O-MIC-WIND-010519/674
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/675
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/676
Information Exposure	08-04-2019	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-010519/677

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	visory/CVE-2019-0755	
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/678
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/679
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/680
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel	https://portal.msrc.microsoft.com/en	O-MIC-WIND-010519/681

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**	-US/security-guidance/advisory/CVE-2019-0767	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/682
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/683

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/684
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/685
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/686
Improper Restriction	09-04-2019	9.3	A remote code execution vulnerability exists when	N/A	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
of XML External Entity Reference ('XXE')			the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**		010519/687
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/688
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/689
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV	N/A	O-MIC-WIND-010519/690

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/691
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/692
Improper Restriction of XML External Entity Reference	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code	N/A	O-MIC-WIND-010519/693

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/694
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/695
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-	N/A	O-MIC-WIND-010519/696

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**		
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**	N/A	O-MIC-WIND-010519/697
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/698
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859.	N/A	O-MIC-WIND-010519/699

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0803		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/700
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0797. **CVE ID : CVE-2019-0808**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0808	O-MIC-WIND-010519/701
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/702
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when	N/A	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 kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0840. **CVE ID : CVE-2019-0844**		010519/703
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/704
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**	N/A	O-MIC-WIND-010519/705
Information	09-04-2019	2.1	An information disclosure vulnerability exists when	N/A	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
Exposure			the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**		010519/706
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/707
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/708
Improper Restriction of Operations within the	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the Windows Graphics Device Interface (GDI) handles objects in	N/A	O-MIC-WIND-010519/709

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			the memory, aka 'GDI+ Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0853**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/710
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/711
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/712

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/713
windows_8.1					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/714

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/715
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/716
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0688**	N/A	O-MIC-WIND-010519/717
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V	https://portal.msrc.microsoft.com/en	O-MIC-WIND-010519/718

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	-US/security-guidance/advisory/CVE-2019-0690	
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/719
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/720
Information	08-04-2019	4	An information disclosure vulnerability exists in the	https://portal.msrc.micr	O-MIC-WIND-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0704	010519/721
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/722
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0731**	N/A	O-MIC-WIND-010519/723
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in	N/A	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 which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**		010519/724
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/725
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/726
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0767,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755	O-MIC-WIND-010519/727

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**		
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/728
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/729
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/730
Information Exposure	08-04-2019	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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767	O-MIC-WIND-010519/731

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted application, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/732
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/733
Information Exposure	08-04-2019	1.9	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-010519/734

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
			'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	visory/CVE-2019-0775	
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/735
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/736
Improper Restriction of XML External Entity Reference	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-010519/737

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/738
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/739
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-	N/A	O-MIC-WIND-010519/740

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/741
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/742
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-	N/A	O-MIC-WIND-010519/743

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/744
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/745
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/746
N/A	09-04-2019	2.1	An elevation of privilege	N/A	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 improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		WIND-010519/747
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797	O-MIC-WIND-010519/748
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/749
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists in Windows when the	N/A	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
			Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**		010519/750
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/751
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/752
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel Information Disclosure	N/A	O-MIC-WIND-010519/753

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0840. **CVE ID : CVE-2019-0844**		
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**	N/A	O-MIC-WIND-010519/754
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/755
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-	N/A	O-MIC-WIND-010519/756

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0879. **CVE ID : CVE-2019-0847**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**	N/A	O-MIC-WIND-010519/757
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/758
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/759

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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'. **CVE ID : CVE-2019-0853**	N/A	O-MIC-WIND-010519/760
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/761
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/762
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-	N/A	O-MIC-WIND-010519/763

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/764
windows_rt_8.1					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/765

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/766
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/767
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure	N/A	O-MIC-WIND-010519/768

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0688**		
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/769
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/770
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/771

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0704		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/772
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0731**	N/A	O-MIC-WIND-010519/773
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'.	N/A	O-MIC-WIND-010519/774

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0732		
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/775
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/776
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755	O-MIC-WIND-010519/777
Improper Restriction of XML External	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010519/778

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Entity Reference ('XXE')			processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	guidance/advisory/CVE-2019-0756	
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/779
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/780
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767	O-MIC-WIND-010519/781

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0782. **CVE ID : CVE-2019-0767**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/782
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/783
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/784

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0782. **CVE ID : CVE-2019-0775**		
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/785
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/786
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**	N/A	O-MIC-WIND-010519/787

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/788
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/789
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**	N/A	O-MIC-WIND-010519/790

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/791
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/792
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**	N/A	O-MIC-WIND-010519/793
Improper Restriction of XML	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core	N/A	O-MIC-WIND-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
External Entity Reference ('XXE')			Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**		010519/794
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/795
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/796
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-010519/797

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797	O-MIC-WIND-010519/798
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/799
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-010519/800

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/801
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/802
Information Exposure	09-04-2019	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-2019-0840. **CVE ID : CVE-2019-0844**	N/A	O-MIC-WIND-010519/803
Improper	09-04-2019	9.3	A remote code execution	N/A	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
Input Validation			vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**		WIND-010519/804
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/805
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**	N/A	O-MIC-WIND-010519/806
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component	N/A	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
			improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**		010519/807
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/808
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/809
Improper Restriction of Operations within the Bounds of a	09-04-2019	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+	N/A	O-MIC-WIND-010519/810

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Buffer			Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0853**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/811
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/812
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/813
Improper	09-04-2019	7.2	A remote code execution	N/A	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
Restriction of Operations within the Bounds of a Memory Buffer			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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**		WIND-010519/814
windows_server_2008					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/815

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/816
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/817
N/A	08-04-2019	4.3	An elevation of privilege vulnerability exists in Active Directory Forest trusts due to a default setting that lets an attacker in the trusting forest request delegation of a TGT for an identity from the trusted forest, aka 'Active Directory Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0683**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0683	O-MIC-WIND-010519/818

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690	O-MIC-WIND-010519/819
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/820
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/821

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0703		
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/822
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/823
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841.	N/A	O-MIC-WIND-010519/824

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0731		
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**	N/A	O-MIC-WIND-010519/825
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/826
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/827
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-010519/828

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	2019-0755	
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/829
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/830
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/831
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel improperly initializes	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010519/832

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**	guidance/advisory/CVE-2019-0767	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/833
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/834

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/835
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/836
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/837
Improper Restriction	09-04-2019	9.3	A remote code execution vulnerability exists when	N/A	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
of XML External Entity Reference ('XXE')			the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**		010519/838
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/839
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**	N/A	O-MIC-WIND-010519/840
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler	N/A	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
			improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**		010519/841
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/842
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**	N/A	O-MIC-WIND-010519/843
Improper Restriction of XML External Entity Reference	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code	N/A	O-MIC-WIND-010519/844

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('XXE')			Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/845
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/846
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-	N/A	O-MIC-WIND-010519/847

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/848
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**	N/A	O-MIC-WIND-010519/849
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836,	N/A	O-MIC-WIND-010519/850

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0841. **CVE ID : CVE-2019-0805**		
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0797. **CVE ID : CVE-2019-0808**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0808	O-MIC-WIND-010519/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/852
Information Exposure	09-04-2019	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-2019-0840. **CVE ID : CVE-2019-0844**	N/A	O-MIC-WIND-010519/853
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface	N/A	O-MIC-WIND-010519/854

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/855
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**	N/A	O-MIC-WIND-010519/856
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka	N/A	O-MIC-WIND-010519/857

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**		
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/858
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/859
Improper Restriction of Operations within the Bounds of a Memory	09-04-2019	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	N/A	O-MIC-WIND-010519/860

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Vulnerability'. **CVE ID : CVE-2019-0853**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/861
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/862
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/863
Improper Restriction	09-04-2019	7.2	A remote code execution vulnerability exists when	N/A	O-MIC-WIND-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**		010519/864
windows_server_2012					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP Server Remote Code	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/865

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/866
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/867
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0688**	N/A	O-MIC-WIND-010519/868
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly	https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-010519/869

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	visory/CVE-2019-0690	
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/870
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/871
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles	https://portal.msrc.microsoft.com/en-US/security-	O-MIC-WIND-010519/872

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	guidance/advisory/CVE-2019-0704	
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/873
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0731**	N/A	O-MIC-WIND-010519/874
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to	N/A	O-MIC-WIND-010519/875

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**		
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/876
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/877
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755	O-MIC-WIND-010519/878

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0782. **CVE ID : CVE-2019-0755**		
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/879
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/880
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/881
Information Exposure	08-04-2019	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	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767	O-MIC-WIND-010519/882

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/883
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/884
Information Exposure	08-04-2019	1.9	An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory, aka 'Windows Kernel	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	O-MIC-WIND-010519/885

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	2019-0775	
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/886
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/887
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from	N/A	O-MIC-WIND-010519/888

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/889
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/890
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-	N/A	O-MIC-WIND-010519/891

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/892
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/893
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795.	N/A	O-MIC-WIND-010519/894

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0792		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/895
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/896
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/897
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when	N/A	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 improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		010519/898
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797	O-MIC-WIND-010519/899
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/900
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to	N/A	O-MIC-WIND-010519/901

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/902
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**	N/A	O-MIC-WIND-010519/903
Information Exposure	09-04-2019	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	N/A	O-MIC-WIND-010519/904

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0840. **CVE ID : CVE-2019-0844**		
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**	N/A	O-MIC-WIND-010519/905
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/906
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-	N/A	O-MIC-WIND-010519/907

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0879. **CVE ID : CVE-2019-0847**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**	N/A	O-MIC-WIND-010519/908
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/909
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**	N/A	O-MIC-WIND-010519/910

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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'. **CVE ID : CVE-2019-0853**	N/A	O-MIC-WIND-010519/911
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/912
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/913
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-	N/A	O-MIC-WIND-010519/914

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/915
windows_server_2016					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/916

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/917
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'. **CVE ID : CVE-2019-0617**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/918
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0682	O-MIC-WIND-010519/919

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0689, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0682**		
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0803, CVE-2019-0859. **CVE ID : CVE-2019-0685**	N/A	O-MIC-WIND-010519/920
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0688**	N/A	O-MIC-WIND-010519/921
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0692, CVE-2019-0693, CVE-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0689	O-MIC-WIND-010519/922

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2019-0694. **CVE ID : CVE-2019-0689**		
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690	O-MIC-WIND-010519/923
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0692**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0692	O-MIC-WIND-010519/924
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0693	O-MIC-WIND-010519/925

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0694. **CVE ID : CVE-2019-0693**		
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0693. **CVE ID : CVE-2019-0694**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0694	O-MIC-WIND-010519/926
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0701. **CVE ID : CVE-2019-0695**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0695	O-MIC-WIND-010519/927
N/A	08-04-2019	7.2	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-010519/928

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Privilege Vulnerability'. **CVE ID : CVE-2019-0696**	2019-0696	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0698, CVE-2019-0726. **CVE ID : CVE-2019-0697**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697	O-MIC-WIND-010519/929
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0726. **CVE ID : CVE-2019-0698**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0698	O-MIC-WIND-010519/930
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0701	O-MIC-WIND-010519/931

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0690, CVE-2019-0695. **CVE ID : CVE-2019-0701**		
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/932
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/933
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/934

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0704		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0698. **CVE ID : CVE-2019-0726**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726	O-MIC-WIND-010519/935
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/936
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836,	N/A	O-MIC-WIND-010519/937

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0841. **CVE ID : CVE-2019-0731**		
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**	N/A	O-MIC-WIND-010519/938
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/939
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754	O-MIC-WIND-010519/940
Information Exposure	08-04-2019	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-010519/941

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	visory/CVE-2019-0755	
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/942
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/943
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	O-MIC-WIND-010519/944
N/A	08-04-2019	7.2	An elevation of privilege vulnerability exists in Windows AppX	https://portal.msrc.microsoft.com/en	O-MIC-WIND-010519/945

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0766**	-US/security-guidance/advisory/CVE-2019-0766	
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767	O-MIC-WIND-010519/946
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666,	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/947

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0667. **CVE ID : CVE-2019-0772**		
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/948
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/949
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0776**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0776	O-MIC-WIND-010519/950
Information Exposure	08-04-2019	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 Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0782	010519/951
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/952
N/A	09-04-2019	7.5	An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file over the SMB protocol on the same machine, aka 'SMB Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0786**	N/A	O-MIC-WIND-010519/953
Improper Restriction of XML External Entity	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka	N/A	O-MIC-WIND-010519/954

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reference ('XXE')			'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/955
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/956
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'.	N/A	O-MIC-WIND-010519/957

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**		
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when DirectX improperly handles objects in memory, aka 'DirectX Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0837**	N/A	O-MIC-WIND-010519/958
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/959
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0838. **CVE ID : CVE-2019-0839**	N/A	O-MIC-WIND-010519/960

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	09-04-2019	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-2019-0844. **CVE ID : CVE-2019-0840**	N/A	O-MIC-WIND-010519/961
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836. **CVE ID : CVE-2019-0841**	N/A	O-MIC-WIND-010519/962
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**	N/A	O-MIC-WIND-010519/963

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/964
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/965
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/966
N/A	09-04-2019	2.1	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV	N/A	O-MIC-WIND-010519/967

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797	O-MIC-WIND-010519/968
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/969
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists in Windows when the Win32k component fails to properly handle objects in memory, aka 'Win32k	N/A	O-MIC-WIND-010519/970

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/971
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0848. **CVE ID : CVE-2019-0814**	N/A	O-MIC-WIND-010519/972
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'.	N/A	O-MIC-WIND-010519/973

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0842		
Information Exposure	09-04-2019	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-2019-0840. **CVE ID : CVE-2019-0844**	N/A	O-MIC-WIND-010519/974
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**	N/A	O-MIC-WIND-010519/975
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/976
Improper Restriction	09-04-2019	9.3	A remote code execution vulnerability exists when	N/A	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
of Operations within the Bounds of a Memory Buffer			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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**		010519/977
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**	N/A	O-MIC-WIND-010519/978
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/979
Improper Restriction of Operations within the	09-04-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database Engine improperly handles objects in memory, aka 'Jet	N/A	O-MIC-WIND-010519/980

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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'. **CVE ID : CVE-2019-0853**	N/A	O-MIC-WIND-010519/981
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/982
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**	N/A	O-MIC-WIND-010519/983

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/984
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/985
windows_server_2019					
N/A	08-04-2019	8.5	A remote code execution vulnerability exists in the way that Windows Deployment Services TFTP Server handles objects in memory. An attacker who successfully exploited the vulnerability could execute arbitrary code with elevated permissions on a	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603	O-MIC-WIND-010519/986

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			target system. To exploit the vulnerability, an attacker could create a specially crafted request, causing Windows to execute arbitrary code with elevated permissions. The security update addresses the vulnerability by correcting how Windows Deployment Services TFTP Server handles objects in memory, aka 'Windows Deployment Services TFTP Server Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0603**		
Information Exposure	08-04-2019	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-2019-0774. **CVE ID : CVE-2019-0614**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614	O-MIC-WIND-010519/987
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	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'.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617	O-MIC-WIND-010519/988

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0617		
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0689, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0682**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0682	O-MIC-WIND-010519/989
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-0803, CVE-2019-0859. **CVE ID : CVE-2019-0685**	N/A	O-MIC-WIND-010519/990
Information Exposure	09-04-2019	5	An information disclosure vulnerability exists when the Windows TCP/IP stack improperly handles fragmented IP packets, aka 'Windows TCP/IP Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0688**	N/A	O-MIC-WIND-010519/991
Integer Overflow or	08-04-2019	4.6	An elevation of privilege vulnerability exists due to	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
Wraparound			an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0692, CVE-2019-0693, CVE-2019-0694. **CVE ID : CVE-2019-0689**	osoft.com/en-US/security-guidance/advisory/CVE-2019-0689	010519/992
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V Network Switch on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0695, CVE-2019-0701. **CVE ID : CVE-2019-0690**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690	O-MIC-WIND-010519/993
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0693, CVE-2019-0694.	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0692	O-MIC-WIND-010519/994

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0692		
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0694. **CVE ID : CVE-2019-0693**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0693	O-MIC-WIND-010519/995
Integer Overflow or Wraparound	08-04-2019	4.6	An elevation of privilege vulnerability exists due to an integer overflow in Windows Subsystem for Linux, aka 'Windows Subsystem for Linux Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0682, CVE-2019-0689, CVE-2019-0692, CVE-2019-0693. **CVE ID : CVE-2019-0694**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0694	O-MIC-WIND-010519/996
Improper Input Validation	08-04-2019	5.5	A denial of service vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0695	O-MIC-WIND-010519/997

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is unique from CVE-2019-0690, CVE-2019-0701. **CVE ID : CVE-2019-0695**		
N/A	08-04-2019	7.2	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-2019-0696**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0696	O-MIC-WIND-010519/998
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0698, CVE-2019-0726. **CVE ID : CVE-2019-0697**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697	O-MIC-WIND-010519/999
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0726. **CVE ID : CVE-2019-0698**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0698	O-MIC-WIND-010519/1000
Improper	08-04-2019	5.5	A denial of service	https://port	O-MIC-

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability exists when Microsoft Hyper-V on a host server fails to properly validate input from a privileged user on a guest operating system, aka 'Windows Hyper-V Denial of Service Vulnerability'. This CVE ID is unique from CVE-2019-0690, CVE-2019-0695. **CVE ID : CVE-2019-0701**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0701	WIND-010519/1001
Information Exposure	08-04-2019	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-2019-0755, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0702**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702	O-MIC-WIND-010519/1002
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0704, CVE-2019-0821. **CVE ID : CVE-2019-0703**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703	O-MIC-WIND-010519/1003

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0703, CVE-2019-0821. **CVE ID : CVE-2019-0704**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704	O-MIC-WIND-010519/1004
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.5	A memory corruption vulnerability exists in the Windows DHCP client when an attacker sends specially crafted DHCP responses to a client, aka 'Windows DHCP Client Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0697, CVE-2019-0698. **CVE ID : CVE-2019-0726**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726	O-MIC-WIND-010519/1005
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0730**	N/A	O-MIC-WIND-010519/1006

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0731**	N/A	O-MIC-WIND-010519/1007
N/A	09-04-2019	4.6	A security feature bypass vulnerability exists in Windows which could allow an attacker to bypass Device Guard when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Security Feature Bypass Vulnerability'. **CVE ID : CVE-2019-0732**	N/A	O-MIC-WIND-010519/1008
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when the Windows Client Server Run-Time Subsystem (CSRSS) fails to properly handle objects in memory, aka 'Windows CSRSS Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0735**	N/A	O-MIC-WIND-010519/1009
Improper Restriction of	08-04-2019	4.9	A denial of service vulnerability exists when Windows improperly	https://portal.msrc.microsoft.com/en	O-MIC-WIND-010519/101

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			handles objects in memory, aka 'Windows Denial of Service Vulnerability'. **CVE ID : CVE-2019-0754**	-US/security-guidance/advisory/CVE-2019-0754	0
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0767, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0755**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755	O-MIC-WIND-010519/1011
Improper Restriction of XML External Entity Reference ('XXE')	08-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0756**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756	O-MIC-WIND-010519/1012
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows Print Spooler does not properly handle objects in memory, aka 'Windows Print Spooler Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0759**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759	O-MIC-WIND-010519/1013
Improper	08-04-2019	9.3	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
Restriction of Operations within the Bounds of a Memory Buffer			vulnerability exists in the way that comctl32.dll handles objects in memory, aka 'Comctl32 Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0765**	al.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765	WIND-010519/1014
N/A	08-04-2019	7.2	An elevation of privilege vulnerability exists in Windows AppX Deployment Server that allows file creation in arbitrary locations. To exploit the vulnerability, an attacker would first have to log on to the system, aka 'Microsoft Windows Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0766**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0766	O-MIC-WIND-010519/1015
Information Exposure	08-04-2019	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-2019-0702, CVE-2019-0755, CVE-2019-0775, CVE-2019-0782. **CVE ID : CVE-2019-0767**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767	O-MIC-WIND-010519/1016

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0665, CVE-2019-0666, CVE-2019-0667. **CVE ID : CVE-2019-0772**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772	O-MIC-WIND-010519/1017
Information Exposure	08-04-2019	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-2019-0614. **CVE ID : CVE-2019-0774**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774	O-MIC-WIND-010519/1018
Information Exposure	08-04-2019	1.9	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-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0782. **CVE ID : CVE-2019-0775**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775	O-MIC-WIND-010519/1019

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. **CVE ID : CVE-2019-0776**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0776	O-MIC-WIND-010519/1020
Information Exposure	08-04-2019	2.1	An information disclosure vulnerability exists when the Windows kernel fails to properly initialize a memory address, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0702, CVE-2019-0755, CVE-2019-0767, CVE-2019-0775. **CVE ID : CVE-2019-0782**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782	O-MIC-WIND-010519/1021
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-04-2019	7.6	A remote code execution vulnerability exists in the way that the ActiveX Data objects (ADO) handles objects in memory, aka 'Windows ActiveX Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0784**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784	O-MIC-WIND-010519/1022
N/A	09-04-2019	7.5	An elevation of privilege vulnerability exists in the Microsoft Server Message Block (SMB) Server when an attacker with valid credentials attempts to open a specially crafted file	N/A	O-MIC-WIND-010519/1023

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			over the SMB protocol on the same machine, aka 'SMB Server Elevation of Privilege Vulnerability'. **CVE ID : CVE-2019-0786**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0791, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0790**	N/A	O-MIC-WIND-010519/1024
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0792, CVE-2019-0793, CVE-2019-0795. **CVE ID : CVE-2019-0791**	N/A	O-MIC-WIND-010519/1025
Information Exposure	08-04-2019	4	An information disclosure vulnerability exists in the way that the Windows SMB Server handles certain requests, aka 'Windows SMB Information Disclosure Vulnerability'. This CVE ID	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821	O-MIC-WIND-010519/1026

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-0703, CVE-2019-0704. **CVE ID : CVE-2019-0821**		
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0841. **CVE ID : CVE-2019-0836**	N/A	O-MIC-WIND-010519/1027
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when Windows Task Scheduler improperly discloses credentials to Windows Credential Manager, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0839. **CVE ID : CVE-2019-0838**	N/A	O-MIC-WIND-010519/1028
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the Terminal Services component improperly discloses the contents of its memory, aka 'Windows Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-010519/1029

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0838. **CVE ID : CVE-2019-0839**		
Information Exposure	09-04-2019	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-2019-0844. **CVE ID : CVE-2019-0840**	N/A	O-MIC-WIND-010519/1030
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists when Windows AppX Deployment Service (AppXSVC) improperly handles hard links, aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0805, CVE-2019-0836. **CVE ID : CVE-2019-0841**	N/A	O-MIC-WIND-010519/1031
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-	N/A	O-MIC-WIND-010519/1032

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0793, CVE-2019-0795. **CVE ID : CVE-2019-0792**		
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0795. **CVE ID : CVE-2019-0793**	N/A	O-MIC-WIND-010519/1033
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9.3	A remote code execution vulnerability exists when OLE automation improperly handles objects in memory, aka 'OLE Automation Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0794**	N/A	O-MIC-WIND-010519/1034
Improper Restriction of XML External Entity Reference ('XXE')	09-04-2019	9.3	A remote code execution vulnerability exists when the Microsoft XML Core Services MSXML parser processes user input, aka 'MS XML Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0790, CVE-2019-0791, CVE-2019-0792, CVE-2019-0793. **CVE ID : CVE-2019-0795**	N/A	O-MIC-WIND-010519/1035
N/A	09-04-2019	2.1	An elevation of privilege	N/A	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 improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0805, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0796**		WIND-010519/1036
N/A	08-04-2019	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'. This CVE ID is unique from CVE-2019-0808. **CVE ID : CVE-2019-0797**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797	O-MIC-WIND-010519/1037
Information Exposure	09-04-2019	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-2019-0849. **CVE ID : CVE-2019-0802**	N/A	O-MIC-WIND-010519/1038
N/A	09-04-2019	7.2	An elevation of privilege vulnerability exists in Windows when the	N/A	O-MIC-WIND-010519/103

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Win32k component fails to properly handle objects in memory, aka 'Win32k Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0685, CVE-2019-0859. **CVE ID : CVE-2019-0803**		9
N/A	09-04-2019	4.6	An elevation of privilege vulnerability exists when Windows improperly handles calls to the LUAFV driver (luafv.sys), aka 'Windows Elevation of Privilege Vulnerability'. This CVE ID is unique from CVE-2019-0730, CVE-2019-0731, CVE-2019-0796, CVE-2019-0836, CVE-2019-0841. **CVE ID : CVE-2019-0805**	N/A	O-MIC-WIND-010519/1040
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0848. **CVE ID : CVE-2019-0814**	N/A	O-MIC-WIND-010519/1041
Improper Restriction of Operations within the Bounds of a	09-04-2019	9.3	A remote code execution vulnerability exists in the way that the VBScript engine handles objects in memory, aka 'Windows VBScript Engine Remote	N/A	O-MIC-WIND-010519/1042

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 Buffer			Code Execution Vulnerability'. **CVE ID : CVE-2019-0842**		
Information Exposure	09-04-2019	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-2019-0840. **CVE ID : CVE-2019-0844**	N/A	O-MIC-WIND-010519/1043
Improper Input Validation	09-04-2019	9.3	A remote code execution vulnerability exists when the IOleCvt interface renders ASP webpage content, aka 'Windows IOleCvt Interface Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0845**	N/A	O-MIC-WIND-010519/1044
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0847, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0846**	N/A	O-MIC-WIND-010519/1045

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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-2019-0846, CVE-2019-0851, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0847**	N/A	O-MIC-WIND-010519/1046
Information Exposure	09-04-2019	2.1	An information disclosure vulnerability exists when the win32k component improperly provides kernel information, aka 'Win32k Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-0814. **CVE ID : CVE-2019-0848**	N/A	O-MIC-WIND-010519/1047
Information Exposure	09-04-2019	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-2019-0802. **CVE ID : CVE-2019-0849**	N/A	O-MIC-WIND-010519/1048
Improper Restriction of	09-04-2019	9.3	A remote code execution vulnerability exists when the Windows Jet Database	N/A	O-MIC-WIND-010519/104

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Engine improperly handles objects in memory, aka 'Jet Database Engine Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-0846, CVE-2019-0847, CVE-2019-0877, CVE-2019-0879. **CVE ID : CVE-2019-0851**		9
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	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'. **CVE ID : CVE-2019-0853**	N/A	O-MIC-WIND-010519/1050
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	9	A remote code execution vulnerability exists when Windows improperly handles objects in memory, aka 'Windows Remote Code Execution Vulnerability'. **CVE ID : CVE-2019-0856**	N/A	O-MIC-WIND-010519/1051
N/A	09-04-2019	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'. This CVE ID is unique from CVE-2019-	N/A	O-MIC-WIND-010519/1052

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0685, CVE-2019-0803. **CVE ID : CVE-2019-0859**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0879. **CVE ID : CVE-2019-0877**	N/A	O-MIC-WIND-010519/1053
Improper Restriction of Operations within the Bounds of a Memory Buffer	09-04-2019	7.2	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-2019-0846, CVE-2019-0847, CVE-2019-0851, CVE-2019-0877. **CVE ID : CVE-2019-0879**	N/A	O-MIC-WIND-010519/1054
Mikrotik					
routeros					
Improper Limitation of a Pathname to a Restricted Directory	10-04-2019	7.5	MikroTik RouterOS versions Stable 6.43.12 and below, Long-term 6.42.12 and below, and Testing 6.44beta75 and below are vulnerable to an	N/A	O-MIK-ROUT-010519/1055

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			authenticated, remote directory traversal via the HTTP or Winbox interfaces. An authenticated, remote attack can use this vulnerability to read and write files outside of the sandbox directory (/rw/disk). **CVE ID : CVE-2019-3943**		
Moxa					
eds-405a_firmware					
N/A	15-04-2019	5	Moxa IKS-G6824A series Versions 4.5 and prior, EDS-405A series Version 3.8 and prior, EDS-408A series Version 3.8 and prior, and EDS-510A series Version 3.8 and prior use plaintext transmission of sensitive data, which may allow an attacker to capture sensitive data such as an administrative password. **CVE ID : CVE-2019-6526**	N/A	O-MOX-EDS-- 010519/1056
eds-408a_firmware					
N/A	15-04-2019	5	Moxa IKS-G6824A series Versions 4.5 and prior, EDS-405A series Version 3.8 and prior, EDS-408A series Version 3.8 and prior, and EDS-510A series Version 3.8 and prior use plaintext transmission of	N/A	O-MOX-EDS-- 010519/1057

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive data, which may allow an attacker to capture sensitive data such as an administrative password. **CVE ID : CVE-2019-6526**		
eds-510a_firmware					
N/A	15-04-2019	5	Moxa IKS-G6824A series Versions 4.5 and prior, EDS-405A series Version 3.8 and prior, EDS-408A series Version 3.8 and prior, and EDS-510A series Version 3.8 and prior use plaintext transmission of sensitive data, which may allow an attacker to capture sensitive data such as an administrative password. **CVE ID : CVE-2019-6526**	N/A	O-MOX-EDS--010519/1058
iks-g6824a_firmware					
N/A	15-04-2019	5	Moxa IKS-G6824A series Versions 4.5 and prior, EDS-405A series Version 3.8 and prior, EDS-408A series Version 3.8 and prior, and EDS-510A series Version 3.8 and prior use plaintext transmission of sensitive data, which may allow an attacker to capture sensitive data such as an administrative password. **CVE ID : CVE-2019-6526**	N/A	O-MOX-IKS--010519/1059

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Opensuse					
leap					
N/A	08-04-2019	7.2	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected. **CVE ID : CVE-2019-0211**	N/A	O-OPE-LEAP-010519/1060
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**	N/A	O-OPE-LEAP-010519/1061
Out-of-bounds Read	08-04-2019	4.3	A vulnerability in the Portable Document Format (PDF) scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an	N/A	O-OPE-LEAP-010519/1062

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of proper data handling mechanisms within the device buffer while indexing remaining file data on an affected device. An attacker could exploit this vulnerability by sending crafted PDF files to an affected device. A successful exploit could allow the attacker to cause a heap buffer out-of-bounds read condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1787**		
Improper Input Validation	08-04-2019	4.3	A vulnerability in the Object Linking & Embedding (OLE2) file scanning functionality of Clam AntiVirus (ClamAV) Software versions 0.101.1 and prior could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a lack of proper input and validation checking mechanisms for OLE2 files	N/A	O-OPE-LEAP-010519/1063

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sent an affected device. An attacker could exploit this vulnerability by sending malformed OLE2 files to the device running an affected version ClamAV Software. An exploit could allow the attacker to cause an out-of-bounds write condition, resulting in a crash that could result in a denial of service condition on an affected device. **CVE ID : CVE-2019-1788**		
Improper Input Validation	11-04-2019	5	The XMLTooling library all versions prior to V3.0.4, provided with the OpenSAML and Shibboleth Service Provider software, contains an XML parsing class. Invalid data in the XML declaration causes an exception of a type that was not handled properly in the parser class and propagates an unexpected exception type. **CVE ID : CVE-2019-9628**	N/A	O-OPE-LEAP-010519/1064
Redhat					
enterprise_linux					
Concurrent Execution using Shared Resource with Improper Synchronizat	08-04-2019	6	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to	N/A	O-RED-ENTE-010519/1065

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion ('Race Condition')			authenticate using another username, bypassing configured access control restrictions. **CVE ID : CVE-2019-0217**		
Information Exposure	11-04-2019	3.3	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1. **CVE ID : CVE-2019-3459**	https://people.canonical.com/~ubuntu-security/cve/2019/CVE-2019-3459.html	O-RED-ENTE-010519/1066
Improper Restriction of Operations within the Bounds of a Memory Buffer	11-04-2019	4.9	It was found that the net_dma code in tcp_recvmsg() in the 2.6.32 kernel as shipped in RHEL6 is thread-unsafe. So an unprivileged multi-threaded userspace application calling recvmsg() for the same network socket in parallel executed on ioatdma-enabled hardware with net_dma enabled can leak the memory, crash the host leading to a denial-of-service or cause a random memory corruption. **CVE ID : CVE-2019-3837**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3837	O-RED-ENTE-010519/1067
N/A	09-04-2019	4.4	In systemd before v242-rc4, it was discovered that pam_systemd does not properly sanitize the environment before using the XDG_SEAT variable. It	N/A	O-RED-ENTE-010519/1068

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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 possible for an attacker, in some particular configurations, to set a XDG_SEAT environment variable which allows for commands to be checked against polkit policies using the "allow_active" element rather than "allow_any". **CVE ID : CVE-2019-3842**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	09-04-2019	5.5	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable. **CVE ID : CVE-2019-3880**	N/A	O-RED-ENTE-010519/1069
reolink					
c1_pro_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command	08-04-2019	9	On Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227, an authenticated admin can use the "TestEmail" functionality to inject and run OS commands as root,	N/A	O-REO-C1_P-010519/1070

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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')			as demonstrated by shell metacharacters in the addr1 field. **CVE ID : CVE-2019-11001**		
c2_pro_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-04-2019	9	On Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227, an authenticated admin can use the "TestEmail" functionality to inject and run OS commands as root, as demonstrated by shell metacharacters in the addr1 field. **CVE ID : CVE-2019-11001**	N/A	O-REO-C2_P-010519/1071
rlc-410w_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-04-2019	9	On Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227, an authenticated admin can use the "TestEmail" functionality to inject and run OS commands as root, as demonstrated by shell metacharacters in the addr1 field. **CVE ID : CVE-2019-11001**	N/A	O-REO-RLC--010519/1072
rlc-422w_firmware					
Improper Neutralization of Special Elements used in an OS	08-04-2019	9	On Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227, an authenticated admin can	N/A	O-REO-RLC--010519/1073

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			use the "TestEmail" functionality to inject and run OS commands as root, as demonstrated by shell metacharacters in the addr1 field. **CVE ID : CVE-2019-11001**		
rlc-511w_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	08-04-2019	9	On Reolink RLC-410W, C1 Pro, C2 Pro, RLC-422W, and RLC-511W devices through 1.0.227, an authenticated admin can use the "TestEmail" functionality to inject and run OS commands as root, as demonstrated by shell metacharacters in the addr1 field. **CVE ID : CVE-2019-11001**	N/A	O-REO-RLC--010519/1074
salicru					
slc-20-cube3(5)					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	05-04-2019	4.3	A reflected HTML injection vulnerability on Salicru SLC-20-cube3(5) devices running firmware version cs121-SNMP v4.54.82.130611 allows remote attackers to inject arbitrary HTML elements via a /DataLog.csv?log= or /AlarmLog.csv?log= or /waitlog.cgi?name= or /chart.shtml?data= or /createlog.cgi?name= request.	N/A	O-SAL-SLC--010519/1075

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-10887		
Sonicwall					
sonicos					
Improper Access Control	02-04-2019	4	A vulnerability in SonicWall SonicOS and SonicOSv, allow authenticated read-only admin to leave the firewall in an unstable state by downloading certificate with specific extension. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V). **CVE ID : CVE-2019-7474**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0001	O-SON-SONI-010519/1076
Improper Access Control	02-04-2019	7.5	A vulnerability in SonicWall SonicOS and SonicOSv with management enabled system on specific configuration allow unprivileged user to access advanced routing services. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3,	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0002	O-SON-SONI-010519/1077

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V). **CVE ID : CVE-2019-7475**		
Use of a Broken or Risky Cryptographic Algorithm	02-04-2019	5	A vulnerability in SonicWall SonicOS and SonicOSv TLS CBC Cipher allow remote attackers to obtain sensitive plaintext data when CBC cipher suites are enabled. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V). **CVE ID : CVE-2019-7477**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0003	O-SON-SONI-010519/1078
sonicosv					
Improper Access Control	02-04-2019	4	A vulnerability in SonicWall SonicOS and SonicOSv, allow authenticated read-only admin to leave the firewall	https://psirt.global.sonicwall.com/vuln-detail/SNWL	O-SON-SONI-010519/1079

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in an unstable state by downloading certificate with specific extension. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V). **CVE ID : CVE-2019-7474**	ID-2019-0001	
Improper Access Control	02-04-2019	7.5	A vulnerability in SonicWall SonicOS and SonicOSv with management enabled system on specific configuration allow unprivileged user to access advanced routing services. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V).	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0002	O-SON-SONI-010519/1080

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-7475		
Use of a Broken or Risky Cryptographic Algorithm	02-04-2019	5	A vulnerability in SonicWall SonicOS and SonicOSv TLS CBC Cipher allow remote attackers to obtain sensitive plaintext data when CBC cipher suites are enabled. This vulnerability affected SonicOS Gen 5 version 5.9.1.10 and earlier, Gen 6 version 6.2.7.3, 6.5.1.3, 6.5.2.2, 6.5.3.1, 6.2.7.8, 6.4.0.0, 6.5.1.8, 6.0.5.3-86o and SonicOSv 6.5.0.2-8v_RC363 (VMWARE), 6.5.0.2.8v_RC367 (AZURE), SonicOSv 6.5.0.2.8v_RC368 (AWS), SonicOSv 6.5.0.2.8v_RC366 (HYPER_V). **CVE ID : CVE-2019-7477**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0003	O-SON-SONI-010519/1081
Verizon					
fios_quantum_gateway_g1100_firmware					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	11-04-2019	9	Remote command injection vulnerability in Verizon Fios Quantum Gateway (G1100) firmware version 02.01.00.05 allows a remote, authenticated attacker to execute arbitrary commands on the target device by adding an access control rule for a network object with a crafted hostname.	N/A	O-VER-FIOS-010519/1082

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

Vulnerability Type(s): CSRF- Cross Site Request Forgery; Dir. Trav.- Directory Traversal; +Info- Gain Information; DoS- Denial of 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-2019-3914		
Improper Authentication	11-04-2019	5.4	Authentication Bypass by Capture-replay vulnerability in Verizon Fios Quantum Gateway (G1100) firmware version 02.01.00.05 allows an unauthenticated attacker with adjacent network access to intercept and replay login requests to gain access to the administrative web interface. **CVE ID : CVE-2019-3915**	N/A	O-VER-FIOS-010519/1083
Information Exposure	11-04-2019	5	Information disclosure vulnerability in Verizon Fios Quantum Gateway (G1100) firmware version 02.01.00.05 allows an remote, unauthenticated attacker to retrieve the value of the password salt by simply requesting an API URL in a web browser (e.g. /api). **CVE ID : CVE-2019-3916**	N/A	O-VER-FIOS-010519/1084
Vmware					
esxi					
Out-of-bounds Read	15-04-2019	5.8	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and	https://www.vmware.com/security/advisories/VMSA-2019-0006.html	O-VMW-ESXI-010519/1085

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.x before 10.1.6) updates address an out-of-bounds vulnerability with the vertex shader functionality. Exploitation of this issue requires an attacker to have access to a virtual machine with 3D graphics enabled. Successful exploitation of this issue may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. The workaround for this issue involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. **CVE ID : CVE-2019-5516**		
Out-of-bounds Read	15-04-2019	5.8	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and 10.x before 10.1.6) contain multiple out-of-bounds read vulnerabilities in the shader translator. Exploitation of these issues requires an attacker	https://www.vmware.com/security/advisories/VMSA-2019-0006.html	O-VMW-ESXI-010519/1086

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to have access to a virtual machine with 3D graphics enabled. Successful exploitation of these issues may lead to information disclosure or may allow attackers with normal user privileges to create a denial-of-service condition on their own VM. The workaround for these issues involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. **CVE ID : CVE-2019-5517**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2019	7.2	VMware ESXi (6.7 before ESXi670-201903001, 6.5 before ESXi650-201903001, 6.0 before ESXi600-201903001), Workstation (15.x before 15.0.4, 14.x before 14.1.7), Fusion (11.x before 11.0.3, 10.x before 10.1.6) contain an out-of-bounds read/write vulnerability in the virtual USB 1.1 UHCI (Universal Host Controller Interface). Exploitation of this issue requires an attacker to have access to a virtual machine with a virtual USB controller present. This issue may	N/A	O-VMW-ESXI-010519/1087

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a guest to execute code on the host. **CVE ID : CVE-2019-5518**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-04-2019	7.2	VMware ESXi (6.7 before ESXi670-201903001, 6.5 before ESXi650-201903001, 6.0 before ESXi600-201903001), Workstation (15.x before 15.0.4, 14.x before 14.1.7), Fusion (11.x before 11.0.3, 10.x before 10.1.6) contain a Time-of-check Time-of-use (TOCTOU) vulnerability in the virtual USB 1.1 UHCI (Universal Host Controller Interface). Exploitation of this issue requires an attacker to have access to a virtual machine with a virtual USB controller present. This issue may allow a guest to execute code on the host. **CVE ID : CVE-2019-5519**	N/A	O-VMW-ESXI-010519/1088
Out-of-bounds Read	15-04-2019	4.3	VMware ESXi (6.7 before ESXi670-201904101-SG and 6.5 before ESXi650-201903001), Workstation (15.x before 15.0.3 and 14.x before 14.1.6), Fusion (11.x before 11.0.3 and 10.x before 10.1.6) updates address an out-of-bounds read vulnerability. Exploitation of this issue requires an attacker to	N/A	O-VMW-ESXI-010519/1089

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

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

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have access to a virtual machine with 3D graphics enabled. Successful exploitation of this issue may lead to information disclosure.The workaround for this issue involves disabling the 3D-acceleration feature. This feature is not enabled by default on ESXi and is enabled by default on Workstation and Fusion. **CVE ID : CVE-2019-5520**		
Zyxel					
nas326_firmware					
N/A	09-04-2019	4	A plaintext password vulnerability in the Zyxel NAS 326 through 5.21 allows an elevated privileged user to get the admin password of the device. **CVE ID : CVE-2019-10630**	N/A	O-ZYX-NAS3-010519/1090
Improper Neutralization of Special Elements used in a Command ('Command Injection')	09-04-2019	6.5	Shell Metacharacter Injection in the package installer on Zyxel NAS 326 version 5.21 and below allows an authenticated attacker to execute arbitrary code via multiple different requests. **CVE ID : CVE-2019-10631**	N/A	O-ZYX-NAS3-010519/1091
Improper Limitation of a Pathname	09-04-2019	4	A directory traversal vulnerability in the file browser component on the	N/A	O-ZYX-NAS3-010519/1092

Vulnerability Type(s)	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			Zyxel NAS 326 version 5.21 and below allows a lower privileged user to change the location of any other user's files. **CVE ID : CVE-2019-10632**		
Improper Control of Generation of Code ('Code Injection')	09-04-2019	6.5	An eval injection vulnerability in the Python web server routing on the Zyxel NAS 326 version 5.21 and below allows a remote authenticated attacker to execute arbitrary code via the tjp6jp6y4, simZysh, and ck6fup6 APIs. **CVE ID : CVE-2019-10633**	N/A	O-ZYX-NAS3-010519/1093
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	09-04-2019	3.5	An XSS vulnerability in the Zyxel NAS 326 version 5.21 and below allows a remote authenticated attacker to inject arbitrary JavaScript or HTML via the user, group, and file-share description fields. **CVE ID : CVE-2019-10634**	N/A	O-ZYX-NAS3-010519/1094

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

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